

Représentations linéaires de groupes finis en caractéristique p^r

THÈSE

présentée à la Faculté des Sciences
de l'Université de Genève
pour obtenir le grade de docteur ès sciences

par

JACQUES THÉVENAZ

dé

Bullet (Vaud)

THÈSE No 1911

1979
—

Zurich
Édition Juris
1980



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41545903_0010

Représentations linéaires de groupes finis en caractéristique p^r

THÈSE

présentée à la Faculté des Sciences
de l'Université de Genève
pour obtenir le grade de docteur ès sciences

par

JACQUES THÉVENAZ

de

Bullet (Vaud)

THÈSE No 1911

Zurich
Édition Juris
1980

La faculté des sciences, sur le préavis de Messieurs M. KERVAIRE, professeur ordinaire et directeur de thèse (Section de Mathématiques), P. GABRIEL, professeur (Université de Zürich) et J. BOECHAT, professeur (Université de Lausanne) autorise l'impression de la présente thèse, sans exprimer d'opinion sur les propositions qui y sont énoncées.

GENÈVE, le 13 mars 1979

Thèse No 1911

Le Doyen:

Bernard Levrat



ISBN 3 260 04809 X

Table des matières.

Chapitre 1 : Anneaux courts.

§1	Généralités	4
§2	Modules sur un anneau court	5
§3	Extensions d'anneaux courts	8
	Le cas non ramifié	10
	Le cas totalement ramifié	11
§4	Théorèmes de structure	13

Chapitre 2 : Représentations de groupes finis sur un anneau court

§1	Généralités	18
§2	Extension des scalaires	19
§3	Modules relativement projectifs	24
§4	Questions de relèvement	30
§5	Enveloppes injectives et couvertures projectives	33

Chapitre 3 : Modules relativement projectifs et représentations non modulaires.

§1	Modules projectifs et blocs	41
§2	Classification des modules relativement projectifs	43
§3	Représentations non modulaires	44
§4	Décomposition en blocs et extension des scalaires	47

Chapitre 4 : Représentations modulaires de groupes cycliques

§1	Représentations modulaires	51
§2	Les types de AC_p -modules	53
§3	Classification des modules de type k	61
§4	Endomorphisme caractéristique global	69
§5	Décomposition en types	71
§6	Classification des AC_p -modules	78
§7	Le groupe cyclique C_2	83

§ 8	Extension des scalaires	87
§ 9	Modules duals et bicompléments	89
§ 10	Modules cohomologiquement triviaux	92
§ 11	Modules de type k par Ext	95
§ 12	Groupes à p -Sylow cyclique	100

Chapitre 5 : Groupes de Grothendieck.

§ 1	Généralités	102
§ 2	$R_A(C)_p$	104
§ 3	Opérations d'Adams	116

<u>Bibliographie</u>	123
----------------------	-----

Introduction

Dans l'étude des représentations entières d'un groupe fini G , on suppose généralement que les $\mathbb{Z}$ -modules sur lesquels G agit sont libres (de type fini). On se propose d'étudier le cas où G agit sur des $\mathbb{Z}$ -modules de torsion, c'est-à-dire des groupes abéliens finis. Cette circonstance apparaît de manière naturelle dans bien des domaines : action d'un groupe de Galois sur un groupe de classes d'idéaux, action d'un groupe fini par transformations de revêtement sur des groupes d'homologie d'espaces, extensions de groupes finis, cohomologie des groupes finis, etc. Même si le module sur lequel le groupe agit n'est pas fini, on obtient une action du type considéré en se restreignant à la $\mathbb{Z}$ -torsion, pour autant qu'elle soit finie. Si en revanche le module est fini mais le groupe ne l'est pas, alors le groupe des automorphismes du module est fini si bien qu'on obtient une action d'un groupe fini en passant au quotient par le noyau de l'action. C'est le cas par exemple en théorie des noeuds où la $\mathbb{Z}$ -torsion des modules de noeuds est finie et où le groupe est cyclique infini.

Historiquement, il faut citer tout d'abord K. Shoda qui, en 1928, a étudié le groupe des automorphismes d'un groupe abélien fini $[\text{Sh}]$. Le problème explicitement posé des représentations d'un groupe fini comme groupe d'automorphismes d'un groupe abélien fini apparaît beaucoup plus tard en liaison avec d'autres questions. Ainsi, G. Szekeres étudie ce problème pour obtenir une classification de certains groupes métabéliens $[\text{Sz}]$ et A. Fröhlich y est amené pour l'étude des groupes de classes d'idéaux de corps de nombres $[\text{Fr}]$. Au début des années 60, V.S. Drobotenko et plusieurs autres Russes s'intéressent aux représentations de groupes finis sur un anneau de classes résiduelles d'entiers. Ils obtiennent des résultats sur la finitude du nombre des indécomposables $[\text{DL}]$ et $[\text{GL}]$ ainsi qu'une classification des représentations du groupe cyclique d'ordre p sur l'anneau $\mathbb{Z}/p^r\mathbb{Z}$ $[\text{DOP}]$. Dans sa thèse, T. Hannula généralise ce dernier résultat à un anneau A/p^rA , quotient d'un anneau de valuation discrète A d'uniformisante p , et étudie le produit tensoriel de ces représentations $[\text{Ha 1 et 2}]$. Signalons aussi que quelques résultats, n'utilisant que des techniques de théorie des groupes finis, sont énoncés dans le livre de Gorenstein $[\text{Go, chap 5, §2}]$.

Si un groupe fini G agit linéairement sur un groupe abélien fini M , les p -composantes M_p de M sont invariantes par G et donc M admet une décomposition G -invariante $M = \bigoplus_p M_p$. Par conséquent on peut supposer que M est un p -groupe, et s'il est d'exposant p^r , on peut considérer M comme un $\mathbb{Z}/p^r\mathbb{Z}$ -module. On est ainsi ramené à l'étude des représentations de G sur l'anneau $\mathbb{Z}/p^r\mathbb{Z}$, c'est-à-dire aux $\mathbb{Z}/p^r\mathbb{Z}[G]$ -modules de type fini. Comme en théorie classique des représentations, les extensions de l'anneau de base $\mathbb{Z}/p^r\mathbb{Z}$ jouent un rôle important dans les questions de décomposition des représentations. On est ainsi conduit à considérer des anneaux jouissant des mêmes propriétés que $\mathbb{Z}/p^r\mathbb{Z}$ et que nous avons appelés pour simplifier les anneaux courts : ce sont les anneaux locaux d'idéal maximal principal engendré par un élément nilpotent.

Le premier chapitre est consacré aux anneaux courts : classification des modules sur un anneau court, extensions d'anneaux courts et ramification, et finalement le théorème qui affirme que tout anneau court est un quotient d'un anneau de valuation discrète ainsi que des théorèmes d'existence et d'unicité d'anneaux courts à corps résiduel donné. Dans un second chapitre sont mis en place les outils principaux utilisés pour la théorie des représentations sur un anneau court : extension des scalaires, modules relativement projectifs, enveloppes injectives et couvertures projectives, compléments de modules. Le troisième chapitre traite de la classification des modules relativement projectifs, de laquelle il résulte la classification de toutes les représentations dans le cas non-modulaire, c'est-à-dire le cas où la caractéristique de l'anneau est première à l'ordre du groupe. La situation est tout à fait semblable à celle des représentations sur un corps : on obtient par exemple un théorème analogue à celui de Wedderburn sur la décomposition en produit d'algèbres de matrices de l'algèbre AG du groupe G sur l'anneau court A . Le cas modulaire est abordé au chapitre 4 pour des anneaux courts dont l'idéal maximal est engendré par le nombre premier p (non ramification). On montre tout d'abord que le nombre des indécomposables n'est jamais fini avant d'aborder les représentations du groupe cyclique d'ordre p^s . Des résultats partiels sont obtenus, en particulier la classification de certains types de modules à l'aide d'un "endomorphisme caractéristique". On parvient à une classification complète dans le cas du groupe cyclique d'ordre p , sous la restriction que les modules sont libres sur l'anneau de base, retrouvant là les résultats de Drobotenko et Hannula. Quelques résultats complémentaires sont exposés dans les derniers paragraphes, en particulier une interprétation des classifications précédentes en termes d'algèbre homologique.

Le dernier chapitre est une digression du côté des groupes de Grothendieck des représentations considérées dans les chapitres 3 et 4 : calcul de ces groupes ainsi que des opérations d'Adams sur ces groupes.

J'adresse mes remerciements à M. Michel Kervaire pour l'aide constante qu'il m'a apportée dans l'élaboration de cette thèse. Mes remerciements vont aussi à MM. Pierre Gabriel, Jacques Boéchat et Charles Kratzer pour les indications précieuses qu'ils m'ont fournies à plusieurs reprises.

Enfin, j'exprime toute ma gratitude à Mlle D. Gay qui a su mener à bien la tâche ingrate de dactylographie.

CHAPITRE 1 : ANNEAUX COURTS

§1 Généralités

Un anneau commutatif A est dit court s'il est local et si l'unique idéal maximal de A est principal engendré par un élément nilpotent π . Exiger que π soit nilpotent est équivalent à imposer que A soit artinien. Il résulte en effet immédiatement de la définition que A ne possède qu'une seule chaîne d'idéaux $A \supset \pi A \supset \pi^2 A \supset \dots \supset \pi^{r-1} A \supset \pi^r A = 0$. Réciproquement, si A est artinien, la suite $A \supset \pi A \supset \pi^2 A \supset \dots$ est stationnaire et il existe donc r tel que $\pi^r A = \pi^{r+1} A$. $\pi^r = \pi^{r+1} a$, $1 - \pi a$ est inversible car A est local et de $\pi^r(1 - \pi a) = 0$, il résulte que $\pi^r = 0$. Le plus petit entier r tel que $\pi^r = 0$ est appelé la longueur de A . Le générateur π de l'idéal maximal, qui est défini à un inversible près, est appelé une uniformisante de A . Tout élément non nul de A s'écrit de manière unique $\pi^k u$ avec u inversible et $0 \leq k < r$. Si p est la caractéristique du corps résiduel $A/\pi A$, alors $p = p \cdot 1 \in \pi A$ et $p^r = 0$ dans A . Ainsi A est de caractéristique p^s (pour un $s \leq r$), ou en d'autres termes A est une $\mathbb{Z}/p^s \mathbb{Z}$ -algèbre. Un anneau court n'est pas principal au sens ordinaire car non intègre. Signalons ici que tout anneau principal non nécessairement intègre est un produit fini d'anneaux principaux intègres et d'anneaux courts [ZS, chap. IV, §15] .

Clairement, tout quotient non trivial d'un anneau de valuation discrète (i.e. local principal) est un anneau court. On verra plus loin que la réciproque est vraie. Plus généralement, tout quotient d'un anneau de Dedekind D par une puissance d'un idéal premier p est un anneau court. En effet, le localisé D_p de D en p est un anneau de valuation discrète [Se 1, chap I, §3] et $D/p^r \cong D_p/p^r D_p$. Cela fournit de nombreux exemples si l'on prend pour D un anneau d'entiers de corps de nombres.

Remarquons enfin qu'un anneau court est complet pour la topologie π -adique, car cette topologie est discrète. On dispose donc en particulier du lemme de Hensel [Bour, chap III, §4, no 3] .

§2 Modules sur un anneau court

Soit A un anneau court de longueur r et d'uniformisante π . Si M est un A -module, les sous-modules suivants de M jouent un rôle particulièrement important : $\pi^k M = \{\pi^k x \mid x \in M\}$ et $M(\pi^k) = \{x \in M \mid \pi^k x = 0\}$, $0 \leq k \leq r$. On a bien sûr : $\pi^{k+1} M \subset \pi^k M$, $M(\pi^k) \subset M(\pi^{k+1})$ et $M/M(\pi^k) \cong \pi^k M$. De plus, comme A est de longueur r , $\pi^k M \subset M(\pi^{r-k})$ et la proposition suivante nous dit quand il y a égalité.

Proposition 1.1: Soit M un A -module. Les conditions suivantes sont équivalentes

- (i) $\pi^k M = M(\pi^{r-k}) \quad \forall k = 0, \dots, r$ (ii) $\pi^{r-1} M = M(\pi)$
 (iii) M est libre (iv) M est projectif (v) M est injectif

Lemme (Nakayama) : Soit M un A -module (non nécessairement de type fini), N un sous-module.

- a) Si $M = \pi M$, alors $M = 0$ b) Si $M = N + \pi M$, alors $M = N$
 c) Si x_i , $i \in I$ sont des représentants dans M d'une base de $M/\pi M$, alors les x_i engendrent M .

Preuve : a) $M = \pi M = \pi^2 M = \dots = \pi^r M = 0$. b) Par a), M/N est nul.

- c) Si N est le sous-module engendré par les x_i , on a $M = N + \pi M$, donc $M = N$.

Preuve de la proposition : (i) $\Rightarrow$ (ii) et (iii) $\Rightarrow$ (iv) sont évidents.

(ii) $\Rightarrow$ (iii) Soient x_i , $i \in I$, des représentants d'une base de $M/\pi M$. Soit L le module libre de base y_i , $i \in I$, et $\alpha: L \rightarrow M$ défini par $\alpha(y_i) = x_i$. α est surjectif par le lemme et on a une suite exacte $0 \rightarrow N \xrightarrow{\beta} L \xrightarrow{\alpha} M = 0$ où $N = \text{Ker } \alpha$. En tensorisant cette suite par $K = A/\pi A$, la suite reste exacte : $0 \rightarrow N/\pi N \xrightarrow{\bar{\beta}} L/\pi L \xrightarrow{\bar{\alpha}} M/\pi M \rightarrow 0$. En effet, par exactitude à droite du foncteur $K \otimes -$, il suffit de vérifier que $\bar{\beta}$ est injectif : Soit $x \in N$ tel que $\bar{\beta} \bar{x} = 0$ (une barre désignant toujours la réduction mod π). Cela signifie que $x \in \pi L$: $x = \pi y$ pour un $y \in L$. Alors $\alpha(y) = \alpha(x) = 0$ car $x \in N$. Par (ii), $\exists w \in M$ tel que $\alpha(y) = \pi^{r-1} w$. Par surjectivité de α , $w = \alpha(z)$ pour un $z \in L$.

Alors $\alpha(y - \pi^{r-1}z) = 0$ et $y - \pi^{r-1}z \in N$. $x = \pi y = \pi(y - \pi^{r-1}z) \in \pi N$ et par conséquent $\bar{x} = 0$, ce qui montre l'injectivité de $\bar{\beta}$.

Par ailleurs $\bar{\alpha}$ est un isomorphisme par construction des x_i et de L . Ainsi $N/\pi N = 0$ et donc $N = 0$ par le lemme. α est un isomorphisme et M est libre.

(iv) $\Rightarrow$ (i) On a $\pi^k(\oplus_i M_i) = \oplus_i \pi^k M_i$ et $(\oplus_i M_i)(\pi^{r-k}) = \oplus_i M_i(\pi^{r-k})$ donc $\pi^k(\oplus_i M_i) = (\oplus_i M_i)(\pi^{r-k}) \Leftrightarrow \pi^k M_i = M_i(\pi^{r-k}) \forall i$. On peut donc supposer M libre et même libre de rang 1 : $M = A$. Soit $\pi^j u \in A(\pi^{r-k})$ avec u inversible. $\pi^{r+j-k}u = 0$, donc $\pi^{r+j-k} = 0$ ce qui force $j-k \geq 0$. Ainsi $\pi^j u \in \pi^j A \subset \pi^k A$ et $A(\pi^{r-k}) \subset \pi^k A$.

(i) $\Rightarrow$ (v) Il suffit de montrer que tout homomorphisme $u : I \rightarrow M$ où I est un idéal de A peut s'étendre en un homomorphisme $v : A \rightarrow M$. $I = \pi^i A$. $\pi^{r-i}u(\pi^i) = u(\pi^r) = 0$. Donc $u(\pi^i) \in M(\pi^{r-i}) = \pi^i M$, $u(\pi^i) = \pi^i x$ pour un $x \in M$. On définit $v : A \rightarrow M$ par $v(1) = x$ et v est clairement une extension de u .

(v) $\Rightarrow$ (ii) Soit $x \in M(\pi)$ et $I = \pi^{r-1}A$. Soit $u : I \rightarrow M$ défini par $u(\pi^{r-1}) = x$. u est bien défini car $\pi x = 0$. Comme M est injectif, u s'étend en un homomorphisme $v : A \rightarrow M$. Alors $x = u(\pi^{r-1}) = v(\pi^{r-1}) = \pi^{r-1}v(1)$ et $x \in \pi^{r-1}M$. $\square$

Remarque : Il est clair que l'équivalence de (iii) et de (iv) résulte aussi du fait que A est local [Bour, chap. II, §3, no 2] .

Corollaire : Si M est libre, $\pi^j M / \pi^i M \cong \pi^{r+j-i} M$ $0 \leq j \leq i \leq r$. En particulier, $M / \pi^i M \cong \pi^{r-i} M$ et $\pi^j M / \pi^{j+1} M \cong M / \pi M \cong \pi^{r-1} M$.

Preuve : La multiplication par $\pi^{r-1} : \pi^j M \rightarrow \pi^{r+j-i} M$ est surjective de noyau $M(\pi^{r-i}) = \pi^i M$. $\square$

La classification des modules de type fini sur un anneau court peut s'obtenir facilement à l'aide du fait que tout anneau court est un quotient d'un anneau de valuation discrète. (cf §4) On obtient néanmoins le résultat de manière directe à l'aide de la proposition 1.1 :

On appellera rang d'un A-module M la dimension du K-espace vectoriel $M/\pi M$, où $K = A/\pi A$. Il résulte du lemme de Nakayama qu'un module de rang n possède un système de générateurs à n éléments et un tel système est même minimal. En particulier un module de rang 1 est monogène, donc de la forme $A/\pi^i A$.

Théorème 1.2 : Soit A un anneau local de longueur r et d'uniformisante π . Tout A-module M de rang n est somme directe de n A-modules de rang 1. Une telle décomposition est unique à isomorphisme près.

Preuve : On procède par récurrence sur r, le cas $r = 1$ étant trivial car alors $A = K$ est un corps. Si $r > 1$, on suppose d'abord que $\pi^{r-1} M = 0$ auquel cas M peut être considéré comme un $A/\pi^{r-1} A$ -module, donc somme directe de n modules de rang 1 par hypothèse de récurrence. Si $\pi^{r-1} M \neq 0$, on choisit $x \in M$ tel que $\pi^{r-1} x \neq 0$. Alors l'homomorphisme $u : A \rightarrow M$ défini par $u(1) = x$ est de noyau nul, ce qui montre que Ax est un sous-module libre de M. Par la proposition 1.1., Ax est injectif, donc facteur direct dans M : $M = Ax \oplus N$. N est clairement de rang $n-1$, donc somme directe de $n-1$ modules de rang 1 par récurrence sur n. L'unicité à isomorphisme près résulte du théorème de Krull-Schmidt car un module de rang 1 est indécomposable. $\square$

Corollaire 1.3 : Tout A-module M de rang n se décompose en $M = M_1 \oplus \dots \oplus M_r$ où M_i est un $A/\pi^i A$ -module libre de rang n_i et $\sum_{i=1}^r n_i = n$. M_i est unique à isomorphisme près.

Preuve : Tout module de rang 1 est isomorphe à $A/\pi^i A$ pour un certain i. Dans une décomposition de M en somme directe de modules de rang 1, on regroupe tous les facteurs isomorphes à $A/\pi^i A$ en une "composante isotypique" M_i . M_i est alors $A/\pi^i A$ -libre d'un certain rang n_i et clairement $\sum n_i = n$. L'unicité résulte du théorème. $\square$

Remarques : 1) Les M_i ne sont pas univoquement déterminés par M, mais seulement uniques à isomorphisme près. Par exemple $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ ne se décompose pas de manière unique.

2) Le théorème 1.2. reste vrai si on ne suppose pas le module M de type fini (cf. $[\text{CK}]$ et $[\text{Wa}]$).

3) Il résulte du théorème 1.2. que tout A -module est quasi-libre, au sens de A. Bouvier ($[\text{Bouv}]$).

4) Les modules M sur un anneau court jouissent de la propriété remarquable suivante : l'enveloppe injective L de M est isomorphe à la couverture projective de M . Si M est de rang n , alors L est libre de rang n .

§2 Extensions d'anneaux courts

Soit A un anneau court de longueur r et d'uniformisante π , B un anneau court de longueur s et d'uniformisante ρ , contenant A . πB est un idéal de B , donc égal à $\rho^e B$ pour un certain $e \geq 1$.

Lemme 1.4 : (i) $re \geq s > (r-1)e$ (ii) B est un A -module libre $\Leftrightarrow s = re$

Preuve : (i) $\rho^{re} B = \pi^r B = 0$, donc $re \geq s$, $\pi^{r-1} \neq 0$ donc $\rho^{(r-1)} \neq 0$ et $(r-1) < s$.

(ii) On peut supposer $r > 1$ sinon $\pi = 0$, A est un corps et clairement $s = e$.

Par la proposition 1.1., B est A -libre si et seulement si $\pi^{r-1} B = B(\pi)$. Comme π et ρ^e sont associés, $B(\pi) = B(\rho^e)$ et comme B est court, $B(\rho^e) = \rho^{s-e} B$. De plus $\pi^{r-1} B = \rho^{(r-1)e} B$ et ainsi B est A -libre si et seulement si $\rho^{(r-1)} B = \rho^{s-e} B$, ou encore $(r-1)e = s-e$, c'est-à-dire $re = s$. $\square$

On supposera désormais que B est un A -module libre et on dira alors que B est une extension de A . C'est là une définition assez naturelle car si A est un quotient d'un anneau de valuation discrète complet A_0 , $A = A_0 / \pi^r A_0$, et si B_0 est la clôture intégrale de A_0 dans une extension finie du corps des quotients de A_0 , alors B_0 est un anneau de valuation discrète et c'est un A_0 -module libre [Se 1, chap II, §2]. Par conséquent, si $B = B_0 / \pi^r B_0$, B est un anneau court et c'est un A -module libre, donc une extension en sens de la définition. Le rang du A -module B est appelé le degré de l'extension. $\rho B \cap A$ est un idéal premier de A , donc égal à πA . L'injection $A \rightarrow B$ définit par passage au quotient une injection $K = A/\pi A \rightarrow L = B/\rho B$. Le degré $[\bar{L} : K]$ est appelé le degré résiduel de l'extension. Enfin, si $\pi B = \rho^e B$, e est appelé l'indice de ramification de l'extension.

Proposition 1.5 : Soit B une extension de A de degré n , de degré résiduel f et d'indice de ramification e . Alors $n = ef$.

Preuve : Comme B est A -libre de rang n , on voit par tensorisation par $K = A/\pi A$ que $B/\pi B$ est un K -espace vectoriel de dimension n . Tous les quotients de la filtration $B \supset \rho B \supset \dots \supset \rho^e B = \pi B$ sont isomorphes et $B/\rho B$ est de dimension f sur K par hypothèse. Il y a e quotients, chacun de dimension f , donc $n = ef$. $\square$

Un polynôme unitaire $f \in A[X]$ est dit irréductible si dans toute expression $f = gh$, $g, h \in A[X]$, on a soit g , soit h inversible. Si $\bar{f} \in A/\pi A[X]$ désigne la réduction modulo π de f , il revient au même d'exiger que soit $\bar{g}$, soit $\bar{h}$ est inversible. On a en effet le lemme :

Lemme 1.6 : Soit R un anneau commutatif et $\pi \in R$ un élément nilpotent. $x \in R$ est inversible $\iff$ l'image $\bar{x}$ de x dans $R/\pi R$ est inversible.

Preuve : Si x est inversible, $\bar{x}$ l'est aussi. Réciproquement, si x est inversible modulo π , $\exists y, z \in R$ tels que $xy = 1 - \pi z$. Alors :
 $xy(1 + \pi z + \pi^2 z^2 + \dots + \pi^{r-1} z^{r-1}) = 1$ où r est tel que $\pi^r = 0$. $\square$

En particulier, $f \in A[X]$ est inversible si et seulement si $f = a + \pi g$ avec a inversible dans A et $g \in A[X]$.

Avec ces préliminaires, on va pouvoir réaliser à peu de chose près une extension de degré fini d'un anneau court A comme un quotient de $A[X]$ par un polynôme irréductible.

Proposition 1.7 : Soit A un anneau court de longueur r et d'uniformisante π et $f \in A[X]$ un polynôme unitaire dont la réduction modulo π^2 (notée encore $\bar{f}$) est irréductible. Alors $B = A[X]/(f)$ est une extension de A , i.e. B est un anneau court et c'est un A -module libre.

Preuve : Si f est de degré n , B est clairement A -libre de base $1, x, \dots, x^{n-1}$.
 $B/\pi B = K[X]/(\bar{f})$ où $K = A/\pi A$ et $\bar{f}$ désigne la réduction modulo π de f . Si $\bar{f} = \bar{g}\bar{h}$ avec $\bar{g}, \bar{h} \in K[X]$ premiers entre eux, alors, par le lemme de Hensel, il existe $g, h \in A[X]$ tels que $f = gh$. Comme f est irréductible dans $A/\pi^2 A[X]$, il l'est a fortiori dans $A[X]$ et donc soit g , soit h est inversible. Ainsi, à un inversible près, la seule décomposition possible de $\bar{f}$ est $\bar{f} = \bar{g}^e$ avec $\bar{g}$ irréductible dans $K[X]$ et $\bar{g}$ unitaire. Alors $A/\pi B \cong K[X]/(\bar{g})^e$ est un anneau court de

longueur e , d'uniformisante g , et de corps résiduel $L = K[X]/(\bar{g})$. Soit g un représentant de $\bar{g}$ dans $A[X]$. Alors $m = (g, \pi)$ est un idéal maximal de B et c'est le seul car, comme π est nilpotent, $\pi B \subset \text{rad } B$ et tout idéal maximal de B contient πB . Ainsi B est local et il reste à montrer que m est principal.

Si $e = 1$, $m = \pi B$ et on suppose donc $e > 1$. Par récurrence sur $s \leq r$, on montre que $B/\pi^s B$ est un anneau court d'uniformisante g . Le cas $s = 1$ est déjà vu. Si $s > 1$, on pose $A' = A/\pi^s A$ et $B' = B/\pi^s B = A'[X]/(f)$. Comme f est irréductible mod π^2 et que $s \geq 2$, les hypothèses de la proposition sont satisfaites pour l'anneau A' .

Comme $\bar{g}^e = 0$ dans $B'/\pi B'$, $g^e = \pi z$ pour un $z \in B'$. $B'/\pi^{r-1} B'$ est court d'uniformisante g par hypothèse de récurrence, donc $z = \lambda g^k \bmod \pi^{s-1}$, $k \geq 0$, λ inversible. Ainsi $g^e = \pi \lambda g^k$.

Si $k \geq 1$, $g(g^{e-1} - \pi \lambda g^{k-1}) = 0$, i.e. $g(g^{e-1} - \pi \lambda g^{k-1}) = hf$ dans $A'[X]$ pour un certain $h \in A'[X]$. Alors $\bar{g} \bar{g}^{e-1} = \bar{h} \bar{f}$ et comme $\bar{f} = \bar{g}^e$, $\bar{h} = 1$ et h est inversible. $f = (h^{-1}g)(g^{e-1} - \pi \lambda g^{k-1})$. Vu que $e > 1$, aucun des 2 facteurs n'est inversible, ce qui contredit l'irréductibilité de f . Donc $k = 0$, $g^e = \pi \lambda$ et $\pi \in gB'$ car λ est inversible. Finalement B' est local d'idéal maximal gB' , $\bar{g}^e B' = \pi B'$ et $g^{se} = 0$. B est donc court de longueur re et d'uniformisante g , par le cas $s = r$. $\square$

Remarque : L'hypothèse que f est irréductible modulo π^2 ne peut être supprimée, comme le montre l'exemple : $f = X^2 + 9 \in \mathbb{Z}/27\mathbb{Z}[X]$. f est irréductible mais réductible mod 9. Dans ce cas $g = X$, $\pi = 3$, et $B = \mathbb{Z}/27\mathbb{Z}[X]/(f)$ est local d'idéal maximal $(3, X)$. On montre aisément que cet idéal n'est pas principal.

Comme pour les anneaux de valuation discrète [Se 1, chap. I §6] il y a deux cas particuliers spécialement importants, les cas non ramifié et totalement ramifié.

Le cas non ramifié

Une extension B de A est non ramifiée, si l'indice de ramification e est égal à 1 (et donc $n = f$) et si l'extension résiduelle est séparable. Si $f \in A[X]$ est tel que $\bar{f}$ est irréductible et séparable, il résulte immédiatement de la proposition 1.7. que $B = A[X]/(f)$ est une extension non ramifiée de A de degré $n = \deg f$ (f est supposé unitaire) car $B/\pi B = K[X]/(\bar{f})$ est un corps, extension séparable de degré n de K . Réciproquement, on a la proposition suivante :

Proposition 1.8 : Soient A un anneau court de résiduel K et B une extension non ramifiée de A de corps résiduel L. L est une extension monogène de K car séparable : $L = K[\bar{x}]$. Soit $\bar{f}$ le polynôme minimal de $\bar{x}$. Alors $\bar{f}$ se relève en un polynôme unitaire f de degré n, tel que $B \cong A[X]/(f)$.

Preuve : Soit $x \in B$ un représentant de $\bar{x}$ et $f_0 \in A[X]$ le polynôme caractéristique de x sur A. Comme B est A-libre de rang n, f_0 est de degré n et unitaire. On a $f_0(x) = 0$, donc $\bar{f}_0(\bar{x}) = 0$. Comme l'extension est non ramifiée, $[L : K] = n$ et $\bar{f}$ est de degré n. Par conséquent $\bar{f}_0 = \bar{f}$ car $\bar{f}_0$ est aussi de degré n. On pose $f = f_0$ et on définit $\phi : A[X]/(f) \rightarrow B$ par $\phi(x) = x$. $\bar{\phi} : K[X]/(\bar{f}) \rightarrow L$ est alors un isomorphisme ce qui implique que ϕ l'est aussi car $\det \phi \notin \pi A$ vu que $\det \bar{\phi} \neq 0$ et donc $\det \phi$ est inversible. $\square$

Remarquons que dans le cas non ramifié, B est automatiquement A-libre. En effet, par le lemme 1.4. on a $re \geq s > (r-1)e$ et comme $e = 1$, cela impose $re = s$.

Proposition 1.9 : Soit A un anneau court d'uniformisante π et de corps résiduel K. Soit L une extension finie séparable de K. Il existe une extension non ramifiée B de A, d'extension résiduelle L/K et cette extension est unique à isomorphisme près.

Preuve : $L = K[\bar{x}]$. Soit $\bar{f}$ le polynôme minimal de $\bar{x}$ sur K et soit $f \in A[X]$ un représentant de $\bar{f}$. f est irréductible modulo π , donc modulo π^2 , et par la proposition 1.7, $B = A[X]/(f)$ est une extension de A, non ramifiée et de corps résiduel L. $\square$

Le cas totalement ramifié

Une extension B de A est totalement ramifiée si le degré f de l'extension résiduelle est égal à 1 (et donc $n = e$).

Un polynôme $f \in A[X]$ est un polynôme d'Eisenstein s'il est de la forme : $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ avec $a_i \in \pi A \quad \forall i = 0, \dots, n-1$ et $a_0 \notin \pi^2 A$.

Remarquons qu'on ne considère que le cas où la longueur de A est ≥ 2 (donc A n'est pas un corps) sinon la condition $a_0 \notin \pi^2 A$ est contradictoire.

Lemme 1.10 : Un polynôme d'Eisenstein est irréductible.

Preuve : Comme $\bar{f} = X^n$, si $f = gh$, alors $\bar{g} = x^k$ et $\bar{h} = X^{n-k}$ (à un inversible près). Alors $g = X^k \bmod \pi$, $h = X^{n-k} \bmod \pi$ et si k et $n-k$ sont non nuls, le terme constant a_0 appartient à $\pi^2 A$. Ainsi, soit g , soit h est inversible. $\square$

Un polynôme d'Eisenstein f est encore un polynôme d'Eisenstein modulo π^2 et donc la proposition 1.7. s'applique : $B = A[X]/(f)$ est une extension de A et comme $B/\pi B \cong K[X]/(X^n)$, la classe x de X dans B est une uniformisante de B , $\pi B = x^n B$ et B est une extension totalement ramifiée de A .

On a aussi dans ce cas une réciproque :

Proposition 1.11 : Soit B une extension totalement ramifiée de A . Il existe un polynôme d'Eisenstein $f \in A[X]$ tel que $B \cong A[X]/(f)$.

Preuve : Soient π une uniformisante de A et ρ une uniformisante de B . On a $\pi B = \rho^n B$ où n est le degré de l'extension. Soit f le polynôme caractéristique de ρ sur A . Comme B est A -libre de rang n , f est de degré n et unitaire. On a $f(\rho) = 0$, $f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$, $a_i \in A$, $a_i = \pi^{c_i} v_i$, v_i inversible, $r \geq c_i \geq 0$ où r est la longueur de A , supposée ≥ 2 . Comme $\pi B = \rho^n B$, $a_i = \rho^{nc_i} u_i$, avec u_i inversible dans B . On pose $c_n = 0$ et $u_n = 1$ ($a_n = \rho^0 \cdot 1 = 1$). La relation $f(\rho) = 0$ s'écrit alors : $\sum_{i=0}^n u_i \rho^{i+nc_i} = 0$. Le n -ème terme est ρ^n , qui est non nul car $\pi \neq 0$ vu que $r \geq 2$. Ainsi tous les termes de la somme ne sont pas nuls. Soit $k + nc_k$ le minimum des $i + nc_i$ ($i = 0, \dots, n$). Ce minimum est atteint par une autre valeur de i que k , sinon $-u_k \rho^{k+nc_k} = \sum_{i \neq k} u_i \rho^{i+nc_i} \in \rho^{(k+nc_k)+1} B$, ce qui est absurde. Il existe par conséquent $j \neq k$ avec $j+nc_j = k+nc_k$. Si on suppose $k > j$, on a $n \mid k-j$, et comme $0 \leq j < k \leq n$, ceci n'est possible que si $j = 0$ et $k = n$. Vu que $c_n = 0$, il vient $nc_0 = n \leq i+nc_i$, $\forall j=1, \dots, n-1$. Alors $c_0 = 1$ et $c_i \geq 1$ pour $1 \leq i \leq n-1$, c'est-à-dire $a_i \in \pi A$ pour $i = 0, \dots, n-1$ et $a_0 \notin \pi^2 A$, f est un polynôme d'Eisenstein. On définit $\phi : A[X]/(f) \rightarrow B$ par $\phi(X) = \rho$. Alors, $\bar{\phi} : K[X]/(f) \rightarrow B/\pi B$ est un isomorphisme car $\bar{f} = X^n$ et $\pi B = \rho^n B$ et donc ϕ est aussi un isomorphisme. $\square$

Exemple 1.12 : Extension cyclotomique. Soit p un nombre premier et A un anneau court d'uniformisante π . Soit $f(X) = \frac{X^{p^s}-1}{X^{p^{s-1}}-1} = \sum_{k=0}^{p-1} X^{kp^{s-1}}$. Alors $B = A[X]/(f)$ est une extension totalement ramifiée de A , de degré $(p-1)p^{s-1}$ et d'uniformisante $x-1$, où x désigne la classe de X dans B . En effet, comme $X^{p^s}-1 = (X-1)p^{s-1} \bmod p$, $\bar{f} = (X-1)^{(p-1)p^{s-1}}$ et si $g(X) = f(X+1)$, alors $\bar{g} = X^{(p-1)p^{s-1}}$. De plus,

par calcul explicite, on voit que le terme constant de g est p et donc g est un polynôme d'Eisenstein. $A[X]/(g)$ est une extension totalement ramifiée de A , d'uniformisante ω où ω désigne la classe de X . Par l'isomorphisme $A[X]/(g) \xrightarrow{\sim} A[X]/(f)$, ω est envoyé sur $x-1$, ce qui démontre l'assertion.

§ 4 Théorèmes de structure .

Les théorèmes de structure pour les anneaux courts découlent pour l'essentiel des résultats de Cohen pour les anneaux locaux complets $[Co]$. Deux cas se présentent suivant que la caractéristique de l'anneau est ou non égale à celle de son corps résiduel.

Cas d'égale caractéristique .

Soit A un anneau court de corps résiduel K avec $\text{car } A = \text{car } K$. Alors la projection $A \rightarrow K$ admet une section $s : K \rightarrow A$ $[Co, \text{thm } 9]$. s est unique si K est une extension algébrique de $\mathbb{Q}$ ou si K est parfait de caractéristique non nulle $[Co, \text{thm } 10]$. Si l'on note encore K l'image de s et si π est une uniformisante de A , alors $A = K[[\pi]]$. On a en effet le lemme général suivant :

Lemme 1.13 : Soit A un anneau court d'uniformisante π , de longueur r et de corps résiduel K . Soit $s : K \rightarrow A$ un système de représentants de K dans A (s n'est bien sûr pas nécessairement un homomorphisme). Alors tout élément $x \in A$ s'écrit de manière unique $x = s(x_0) + s(x_1)\pi + \dots + s(x_{r-1})\pi^{r-1}$.

Preuve : Si x_0 désigne la classe de x dans K , alors x et $s(x_0)$ ont même image dans K , donc diffèrent par un multiple de π . $x = s(x_0) + y\pi$. La classe x_1 de y dans K est entièrement déterminée par x et on itère le processus. $\square$

En revenant au cas d'égale caractéristique, on a $A = K[[\pi]]$ et comme $\pi^r = 0$, $\pi^{r-1} \neq 0$, $A \cong K[X]/(X^r)$. Si D désigne le localisé de $K[X]$ en X , on a aussi $A \cong D/(X^r)$ et donc A est un quotient d'un anneau de valuation discrète.

Cas d'inégale caractéristique :

Si la caractéristique de K est nulle, celle de A l'est forcément aussi et par conséquent le seul cas d'inégale caractéristique est celui où $\text{car}(K) = p \neq 0$ et $\text{car}(A) = p^s$, $s \geq 2$. On dira alors que A est un p -anneau court. De plus, on appellera p -anneau court non ramifié un p -anneau court admettant p pour uniformisante. Dans ce dernier cas, on a $p^r = 0$, où r est la longueur de A , et A est une $\mathbb{Z}/p^r\mathbb{Z}$ -algèbre, extension non ramifiée de $\mathbb{Z}/p^r\mathbb{Z}$ (non nécessairement

de degré fini). C'est ce cas qui nous intéressera particulièrement dans la suite.

Le résultat clé de la théorie générale de Cohen [Co, thm 11] s'énonce pour les p-anneaux courts de la manière suivante :

Théorème 1.14 : Soit A un p-anneau court de corps résiduel K. Alors il existe un anneau de valuation discrète D d'uniformisante p et de corps résiduel K et un homomorphisme $t : D \rightarrow A$ induisant l'identité de K par passage aux corps résiduels.

Ce théorème garantit donc l'existence d'un p-anneau court non ramifié B ayant même corps résiduel que A et qui est sous-anneau de A. On prend en effet $B = t(D)$. Si s est le plus petit entier tel que $p^s = 0$ ($s \geq 2$), $B \cong D/p^s D$ car $p^s D = \text{Ker } t$. Si A est de longueur r et d'uniformisante π et si $pA = \pi^e A$, alors on a $(s-1)e < r \leq se$ (lemme 1.4.). En prenant un système de représentants de K dans B, on voit à l'aide du lemme 1.13 que $A = B[\pi]$ et que c'est un B-module de type fini. Si A est non ramifié, c'est-à-dire si $e = 1$, alors $B = A$ et A est un quotient d'un anneau de valuation discrète. Montrons que ce dernier résultat reste valable dans le cas ramifié.

Si A est un B-module libre, alors $r = se$ par le lemme 1.4. et A est une extension totalement ramifiée de B de degré e vu que le degré résiduel est 1. Par la proposition 1.11, $A \cong B[X]/(f)$ où f est un polynôme d'Eisenstein. En relevant f en un polynôme d'Eisenstein à coefficients dans D, noté encore f, et en posant $C = D[X]/(f)$, on a $A \cong C/p^s C$. Mais C est un anneau de valuation discrète [Se 1, chap. I, §6]. Plus précisément, si L est le corps des fractions de D, alors C est la clôture intégrale de D dans l'extension $L[X]/(f)$ de L. Reste donc le cas où A n'est pas libre sur B. On a alors $e \geq 2$ et $(s-1)e < r < se$. Nous allons montrer qu'alors A est un quotient d'un p-anneau court A', libre de rang e sur B, donc de longueur se, et le cas précédent s'appliquera. Comme $A = B[\pi]$, on a un homomorphisme surjectif $\phi : B[X] \rightarrow A$ défini par $\phi(X) = \pi$. Par ailleurs $B/p^{s-1}B \subset A/p^{s-1}A = A/\pi^{(s-1)e}A$ et donc $A/p^{s-1}A$ est un $B/p^{s-1}B$ -module 1 en vertu du lemme 1.4. Si Ψ désigne l'homomorphisme induit par ϕ modulo p^{s-1} , $\Psi : B/p^{s-1}B[X] \rightarrow A/p^{s-1}A$, la proposition 1.11 montre dans le cas $s \geq 3$ que $\text{Ker } \Psi = (f)$ où f est un polynôme d'Eisenstein de degré e. Si $s = 2$, $B/p^{s-1}B = K$ et on est dans le cas d'égale caractéristique. Alors $\text{Ker } \Psi = (f)$ où $f = X^e$. Dans les deux cas, nous allons relever f dans $B[X]$ en un polynôme d'Eisenstein g tel que $g \in \text{Ker } \Psi$. Tout d'abord notons encore f un relevé unitaire de f dans B[

On a : $\phi(f) = f(\pi) = 0 \pmod{p^{s-1}}$. $f(\pi) = p^{s-1}a$. Par le lemme 1.13, a s'écrit $a = a_0 + a_1\pi + \dots + a_{r-1}\pi^{r-1}$ où les a_i appartiennent à un système de représentants de K dans B . En effet A et B ont même corps résiduel. Comme $p^{s-1}A = \pi^{(s-1)e}A$, on a $p^{s-1}\pi^i = 0$ pour $i \geq r-(s-1)e$. Donc :

$$f(\pi) = a_0 p^{s-1} + a_1 p^{s-1} \pi + \dots + a_k p^{s-1} \pi^k \text{ où } k = r - (s-1)e - 1. k < e \text{ car } (s-1)e < r < se.$$

Soit $g = f - \sum_{i=0}^k a_i p^{s-1} \pi^i \in \mathfrak{A}[X]$. Le coefficient dominant de g est 1 car $k < e$ et tous les autres coefficients sont multiples de p . Reste à examiner le terme constant.

Si $s = 2$, $f = X^e$ donc $\pi^e = f(\pi) = pa$ et a est inversible vu que π^e et p engendrent le même idéal de A . Cela signifie que a_0 est non nul, donc inversible et, comme le terme constant de g est $-a_0 p$, g est un polynôme d'Eisenstein.

Si $s \geq 3$, f est un polynôme d'Eisenstein et son terme constant est donc de la forme $b_0 p$ avec b_0 inversible. Le terme constant de g est alors $(b_0 - a_0 p^{s-2})p$ qui n'est pas multiple de p^2 . Ainsi dans tous les cas, il existe un polynôme d'Eisenstein $g \in \text{Ker } \phi$ car on a bien sûr $g(\pi) = 0$ par construction. ϕ se factorise donc à travers $B[X]/(g) = A'$ qui est un anneau court, extension totalement ramifiée de B . Comme A' est libre sur B , on a vu que A' est un quotient d'un anneau de valuation discrète C . A étant un quotient de A' , il est aussi un quotient de C . Remarquons que, comme la classe de π est une uniformisante de A' , on a $\text{Ker } \phi = (f, X^r)$. Ainsi nous avons montré le théorème :

Théorème 1.15 : Soit A un anneau court de longueur r , d'uniformisante π et de corps résiduel K . Alors :

- 1) Il existe un anneau de valuation discrète D , d'uniformisante notée aussi π , tel que $A \cong D/\pi^r D$.
- 2) Si A et K ont même caractéristique, $A \cong K[X]/(X^r)$.
- 3) Si A et K n'ont pas même caractéristique, alors A est de caractéristique p^s , pour $s \geq 2$, et si $pA = \pi^e A$ alors :
 - a) A possède un sous-anneau court B non ramifié (i.e. d'uniformisante p) de longueur s et de corps résiduel K . De plus $(s-1)e < r \leq se$.
 - b) $A \cong A'/\pi^r A'$ où A' est un anneau court de longueur se qui est extension totalement ramifiée de degré e de B . Plus précisément, si $A' = B[X](f)$ (f étant un polynôme d'Eisenstein), alors $A \cong B[X](f, X^r)$.

Remarques : 1) Si A est un quotient d'un anneau de Dedekind D par une puissance d'un idéal premier $\mathfrak{p}$, on réalise A comme un quotient d'un anneau de valuation discrète en localisant D en $\mathfrak{p}$ puis en passant au quotient.

2) Dans la première assertion du théorème, on peut aussi supposer D complet (pour sa topologie π -adique) car si $\hat{D}$ désigne le complété de D , on a $\hat{D}/\pi^r \hat{D} = D/\pi^r D$.

Nous allons maintenant examiner les questions d'existence et d'unicité d'anneaux courts à corps résiduel donné. Dans le cas d'égale caractéristique, pour K donné, il existe un et un seul anneau court de longueur r et de corps résiduel $K : K[X]/(X^r)$. On se place donc dans le cas d'inégale caractéristique et la question se réduit à celle de l'existence d'un anneau de valuation discrète D de caractéristique nulle à corps résiduel K de caractéristique p donné. Clairement, toute extension totalement ramifiée d'un tel D fournit un autre anneau de valuation discrète à corps résiduel K . On suppose donc D non ramifié, i.e. d'uniformisante p . Le corps résiduel ne changeant pas non plus par complétion, on suppose enfin D complet. On a alors le théorème suivant, dû à Hasse et Schmidt (cf. [Ma, theorem 2 et theorem 8, corollary 1] ainsi que [La]) :

Théorème 1.16 : Soit K un corps de caractéristique p . Il existe un anneau de valuation discrète complet D non ramifié de corps résiduel K . D est unique à isomorphisme près.

D peut être réalisé comme l'anneau des vecteurs de Witt $W(K)$ (cf. [Se, chap. II, §5-6]). Le quotient $D/p^r D$ est un p -anneau court non ramifié de longueur r , qu'on peut voir aussi comme l'anneau des vecteurs de Witt de longueur r

$W_r(K)$. Par le théorème 1.15, tout p -anneau court non ramifié est un quotient d'un anneau de valuation discrète complet non ramifié. On a donc :

Corollaire 1.17 : Soit K un corps de caractéristique p et r un entier positif. Alors il existe un p -anneau court non ramifié A de longueur r et de corps résiduel K . A est unique à isomorphisme près.

Dans le cas où le corps résiduel est parfait, on a encore le résultat suivant [Se 1, chap. II, prop. 10] :

Proposition 1.18 : Soient D_1 et D_2 deux anneaux de valuation discrète complets non ramifiés de corps résiduels respectifs K_1 et K_2 parfaits. Pour tout homomorphisme $\bar{f} : K_1 \rightarrow K_2$, il existe un homomorphisme $f : D_1 \rightarrow D_2$ et un seul induisant $\bar{f}$ sur les corps résiduels.

Remarque : Si K n'est pas parfait, $\bar{f} : K_1 \rightarrow K_2$ se relève en $f : D_1 \rightarrow D_2$ mais de manière non unique (cf. [Ma, theorem 10]).

Corollaire 1.19 : Soit A un p -anneau court non ramifié de corps résiduel parfait K . Le treillis des extensions non ramifiées de A est isomorphe par réduction modulo p au treillis des extensions finies de K .

Preuve : Une extension finie $\bar{f} : K \rightarrow L$ est séparable. Si B désigne l'unique extension non ramifiée de A d'extension résiduelle L/K (prop. 1.9), l'homomorphisme $\bar{f}$ se relève de manière unique en un homomorphisme injectif $f : A \rightarrow B$ car il se relève même au niveau des anneaux de valuation discrète.

Remarque : Si $\hat{K}$ désigne la clôture algébrique de K et $\hat{A}$ le p -anneau court non ramifié de corps résiduel $\hat{K}$, alors $\hat{A}$ est la "clôture non ramifiée" de A .

CHAPITRE 2 : REPRESENTATIONS DE GROUPES FINIS SUR UN ANNEAU COURT

§1 Généralités

Soit A un anneau court et G un groupe fini. Une représentation de G sur A est la donnée d'un AG -module à gauche de type fini, où AG désigne l'algèbre du groupe G sur A . Comme G est fini, un AG -module de type fini M est aussi de type fini comme A -module et la donnée de M équivaut à la donnée d'un A -module de type fini M et d'un homomorphisme $\phi : G \rightarrow \text{Aut}_A M$. On supposera plus tard que M est un A -module libre, auquel cas on peut voir ϕ comme un homomorphisme de G dans $GL_n(A)$, une fois choisie une A -base de M . On convient une fois pour toutes que tous les AG -modules seront des AG -modules à gauche.

A étant artinien et G fini, AG est artinien comme A -module, donc a fortiori comme anneau. Tout AG -module de type fini est donc de longueur finie et on dispose des théorèmes de Jordan-Hölder et de Krull-Schmidt.

Si τ désigne une uniformisante de A , τ est central dans AG et par conséquent, si M est un AG -module, $\tau^k M$ et $M(\tau^k)$ sont des sous- AG -modules de M . Si M est A -libre, $M(\tau^k) = \tau^{r-k} M$ et $\tau^j M / \tau^i M \cong \tau^{r+j-i} M$ ($0 \leq j \leq i \leq r$) (proposition 1.1 et corollaire).

Proposition 2.1 : Soit $K = A/\tau A$ le corps résiduel de A . Les AG -modules simples s'identifient aux KG -modules simples.

Preuve : Tout KG -module simple reste simple si on le considère comme AG -module. Réciproquement, si M est un AG -module simple, τM est un sous-module de M et donc $\tau M = 0$. M peut être alors considéré comme un KG -module. $\square$

On obtient une suite de Jordan-Hölder d'un AG -module M en raffinant la filtration $M \supset \tau M \supset \tau^2 M \supset \dots \supset \tau^{r-1} M \supset 0$, ce qui revient à choisir une suite de Jordan-Hölder de chaque quotient $\tau^i M / \tau^{i+1} M$, qui est un KG -module.

Rappelons le résultat classique suivant [CR, §14] et [Co, §43].

Proposition 2.2 : Soit R un anneau artinien et M un R -module de type fini. Les conditions suivantes sont équivalentes :

(i) M est indécomposable (ii) Tout endomorphisme de M est soit nilpotent, soit inversible (iii) $\text{End}_R M$ est un anneau local. $\square$

Si M est un AG -module et si $f \in \text{End}_{AG} M$, alors $f(\pi M) \subset \pi M$ et donc f induit $\bar{f} \in \text{End}_{KG} M/\pi M$. Cela définit un homomorphisme : $\phi : \text{End}_{AG} M \rightarrow \text{End}_{KG} M/\pi M$.

Proposition 2.3 : M est indécomposable si et seulement si $\text{Im } \phi$ est un sous-anneau local de $\text{End}_{KG} (M/\pi M)$.

Preuve : Si M est indécomposable, $\text{Im } \phi$ est un anneau local car image d'un anneau local. Réciproquement, si $\mathfrak{m}$ désigne l'image réciproque par ϕ de l'unique idéal maximal de $\text{Im } \phi$, alors le complémentaire de $\mathfrak{m}$ est l'ensemble des éléments inversibles. En effet, si $x \notin \mathfrak{m}$, x est inversible à gauche mod $\text{Ker } \phi$. Or $\text{Ker } \phi$ est un nilidéal car si $f \in \text{Ker } \phi$, $f(M) \subset \pi M$, donc $f^r(M) \subset \pi^r M = 0$, r étant la longueur de l'anneau A . Donc x est inversible à gauche (comme dans le lemme 1.6). De même, x est inversible à droite. $\square$

§2 Extension des scalaires.

Soit A un anneau court de corps résiduel K . Pour simplifier, on appellera extension de A toute extension non ramifiée de A . Si G est un groupe fini et si B est une extension de A , $B \otimes_A^{\vee} AG \cong BG$ et à tout AG -module M , on peut associer $B \otimes_A M$ qui est muni canoniquement d'une structure de BG -module. C'est l'extension des scalaires de A à B .

On se propose d'étudier le comportement des modules indécomposables par extension des scalaires. Un AG -module de type fini M est dit absolument indécomposable si pour toute extension B de A , $B \otimes_A M$ est un BG -module indécomposable.

Proposition 2.4 : Soient M un AG -module de type fini indécomposable, $\mathfrak{m}$ l'unique idéal maximal de $E = \text{End}_{AG} M$ et $D = E/\mathfrak{m}$ le corps résiduel (non nécessairement commutatif). Alors :

- (i) D est une K -algèbre de dimension finie sur K .
- (ii) Si K est parfait, M est absolument indécomposable si et seulement si $D = K$.

Preuve : La multiplication scalaire par un élément $a \in A$ étant un élément de E , on a une injection canonique $A \rightarrow E$, qui induit une injection $K \rightarrow D$. Comme M est de type fini sur A , E est de type fini sur A et par conséquent $[D : K]$ est fini ce qui montre (i).

Pour montrer (ii), on a besoin du fait que $B \otimes_A \text{End}_{AG} M = \text{End}_{BG} (B \otimes_A M)$, ce qui résulte du lemme classique suivant :

Lemme : Soit A un sous-anneau d'un anneau commutatif B . On suppose que B est un A -module plat. Si M et N sont deux AG -modules avec M de présentation finie comme A -module alors $B \otimes_A \text{Hom}_{AG}(M, N) \stackrel{\sim}{=} \text{Hom}_{BG}(B \otimes_A M, B \otimes_A N)$.

Preuve : On montre d'abord que $B \otimes_A \text{Hom}_A(M, N) = \text{Hom}_B(B \otimes_A M, B \otimes_A N)$. Soit

$$h : B \otimes_A \text{Hom}_A(M, N) \rightarrow \text{Hom}_B(B \otimes_A M, B \otimes_A N)$$

$b \otimes f \longmapsto m_b \otimes f$ où m_b désigne la multiplication par b dans B .

Si M est A -libre, on vérifie immédiatement que h est un isomorphisme. Si maintenant $0 \rightarrow K \rightarrow L \rightarrow M \rightarrow 0$ est une présentation de M , on a en vertu de la platitude de B :

$$\begin{array}{ccccc} 0 \rightarrow B \otimes_A \text{Hom}_A(M, N) & \rightarrow & B \otimes_A \text{Hom}_A(L, N) & \rightarrow & B \otimes_A \text{Hom}_A(K, N) \\ & \downarrow h_M & & \downarrow h_L & & \downarrow h_K \\ 0 \rightarrow \text{Hom}_B(B \otimes_A M, B \otimes_A N) & \rightarrow & \text{Hom}_B(B \otimes_A L, B \otimes_A N) & \rightarrow & \text{Hom}_B(B \otimes_A K, B \otimes_A N) \end{array}$$

h_L est un isomorphisme car L est libre et donc h_M est injectif. Comme K est de type fini, le même raisonnement appliqué à une présentation de K montre que h_K est injectif. Mais alors h_M est un isomorphisme par le lemme des cinq.

G agit sur $\text{Hom}_A(M, N)$ par $(g, f)(x) = g f(g^{-1}x)$ et de même sur

$\text{Hom}_B(B \otimes_A M, B \otimes_A N)$. On vérifie que h est un isomorphisme BG -linéaire et le résultat s'ensuit en prenant les invariants dans les deux membres, compte tenu du fait que $[B \otimes_A \text{Hom}_A(M, N)]^G = B \otimes_A \text{Hom}_{AG}(M, N)$. Pour prouver cette dernière égalité, on pose $V = \text{Hom}_A(M, N)$ et on définit $W = \bigoplus_{g \in G} V_g$ où $V_g \stackrel{\sim}{=} V$.

Soit alors $q : V \rightarrow W$

$$x \mapsto \sum_{g \in G} ((g-1)x)_g \quad . \quad q \text{ est } A\text{-linéaire de noyau } V^G.$$

Alors $0 \rightarrow B \otimes_A V^G \rightarrow B \otimes_A V \xrightarrow{1 \otimes q} B \otimes_A W$. Or $\text{Ker}(1 \otimes q) = (B \otimes_A V)^G$ et donc $(B \otimes_A V)^G = B \otimes_A V^G$.

Montrons alors (ii). Si B est une extension de A , B est A -libre et on a $B \otimes_A E \cong \text{End}_{BG}(B \otimes_A M)$ par le lemme. De plus $B \otimes_A D \cong B \otimes_A K \otimes_K D \cong L \otimes_K D$ où L est le corps résiduel de B . En tensorisant par B la suite $0 \rightarrow m \rightarrow E \rightarrow D \rightarrow 0$, on obtient donc $0 \rightarrow B \otimes_A m \rightarrow \text{End}_{BG}(B \otimes_A M) \rightarrow L \otimes_K D \rightarrow 0$.

Si $D = K$, alors $L \otimes_K D = L$. Comme m est nilpotent, $B \otimes_A m$ l'est aussi et donc $B \otimes_A m$ est le radical de $\text{End}_{BG}(B \otimes_A M)$. Ainsi $\text{End}_{BG}(B \otimes_A M)$ est local et $B \otimes_A M$ est indécomposable. Donc M est absolument indécomposable. Réciproquement, si $D \neq K$, soit $x \in D$ avec $x \notin K$. x est séparable sur K car K est parfait. Soit $L = K[x]$ et B l'extension non ramifiée de A d'extension résiduelle L/K . On veut montrer que $B \otimes_A M$ est décomposable. Comme $L \otimes_K D$ est un quotient de $\text{End}_{BG}(B \otimes_A M)$, il suffit de montrer que $L \otimes_K D$ n'est pas local. Comme $L \subset D$, $L \otimes_K L \subset L \otimes_K D$. Si $L = K[x]/(f)$, f se décompose dans L en un produit $g \cdot h$ de polynômes premiers entre eux (séparabilité) et donc $L \otimes_K L \cong L[x]/(f) \cong L[x]/(g) \times L[x]/(h)$. Ainsi $L \otimes_K L$, et à fortiori $L \otimes_K D$, contient 2 idempotents distincts de 1. $L \otimes_K D$ n'est donc pas local. $\square$

Corollaire : M est absolument indécomposable si et seulement si $B \otimes_A M$ est indécomposable pour toute extension finie B de A .

Preuve : On a vu en fin de démonstration que si $D \neq K$, M est décomposé par une extension finie de A . $\square$

Proposition 2.5 : Soit M un AG-module de type fini. M est complètement décomposé par une extension finie de A , i.e. il existe une extension finie B de A telle que chaque facteur indécomposable de $B \otimes_A M$ soit absolument indécomposable.

Preuve : Si B est une extension finie de A , soit m_B le nombre de facteurs indécomposables de $B \otimes_A M$. Si $n = \text{rang}_A M$, on a $1 \leq m_B \leq n$. On choisit B en sorte que m_B soit maximal, ce qui est possible vu que m_B est borné. Alors

m_B reste constant par toute extension finie de B , ce qui signifie que tout facteur indécomposable N de $B \otimes_A M$ reste indécomposable par extension finie des scalaires. Par le corollaire précédent, N est absolument indécomposable. $\square$

Remarques : 1) Il est clair que tout AG -module de type fini est complètement décomposé par la clôture non ramifiée $\bar{A}$ de A . Il est clair aussi que si le nombre des modules indécomposables est fini, tous les modules sont complètement décomposés simultanément par une extension finie de A . On verra au chapitre 3 que c'est le cas si la caractéristique de K ne divise pas l'ordre du groupe. En revanche, pour A un p -anneau court non ramifié et $G = C_p$, seule la clôture non ramifiée de A décompose complètement tous les modules simultanément (propositions 3.13 et 4.30).

2) Si on ne considère que les AG -modules qui sont A -libres, on a aussi une notion de module irréductible, et de même une notion de module absolument irréductible : un AG -module A -libre est irréductible s'il ne possède pas de sous-module A -libre non trivial. Clairement un module (absolument) irréductible est (absolument) indécomposable. Mais d'autres questions se posent. Un module irréductible qui est absolument indécomposable est-il absolument irréductible ? Réciproquement, si tous les facteurs irréductibles d'une "suite de composition" d'un module indécomposable sont absolument irréductibles, le module est-il absolument indécomposable ? Les réponses sont affirmatives dans les deux cas cités dans la 1ère remarque. On a alors une notion d'anneau de décomposition du groupe G comme étant un anneau court A pour lequel tous les AG -modules irréductibles sont absolument irréductibles (ou bien tous les AG -modules indécomposables sont absolument indécomposables). Dans le cas du groupe cyclique C_p , seule une clôture non ramifiée peut être un anneau de décomposition du groupe.

Toujours concernant les extensions de scalaires, on a encore les deux résultats suivants :

Proposition 2.6 : Soient A un anneau court, B une extension finie de A , M et N deux AG -modules de type fini. $M \cong N \iff B \otimes_A M \cong B \otimes_A N$.

Preuve : B étant A -libre, on a $B = e_1 A \oplus \dots \oplus e_n A$ et donc $B \otimes_A M = (e_1 \otimes M) \oplus \dots \oplus (e_n \otimes M) \cong M^n$ comme AG -modules. Si $B \otimes_A M \cong B \otimes_A N$, alors $M^n \cong N^n$ et en décomposant M et N en AG -modules indécomposables, les facteurs

doivent être deux à deux isomorphes à l'ordre près par le théorème de Krull-Schmidt. Donc $M \cong N$. La réciproque est évidente. $\square$

Proposition 2.7 : Soient A un anneau court, B une extension finie de A et M un BG-module de type fini. Alors il existe un AG-module M_0 tel que M soit facteur direct dans $B \otimes_A M_0$. On peut choisir $M_0 = M$ considéré comme AG-module.

Avant d'entamer la preuve, il est nécessaire de faire un peu de théorie de Galois. Si $A = R/\pi^k R$ et $B = S/\pi^k S$ où R et S sont des anneaux de valuation discrète complets et si K et L désignent les corps des fractions de R et S respectivement, alors L est une extension non ramifiée de K, d'extension résiduelle $\bar{L}/\bar{K}$ où $\bar{K} = A/\pi A = R/\pi R$ et $\bar{L} = B/\pi B = S/\pi S$. Supposons L/K galoisienne, et soit $\sigma \in \text{Gal}(L/K)$. σ induit $\sigma: S \rightarrow S$ et comme $\sigma(\pi) = \pi$ car $\pi \in R$, σ induit encore $\bar{\sigma}: \bar{L} \rightarrow \bar{L}$. Cette correspondance fournit un isomorphisme $\text{Gal } L/K \xrightarrow{\sim} \text{Gal } \bar{L}/\bar{K}$ (cf. proposition 1.18 et pour plus de détails [Se 1, chap. III, §5]). L/K est galoisienne si et seulement si $\bar{L}/\bar{K}$ l'est.

Si $\sigma \in \text{Gal } L/K$, σ induit $\sigma: B \rightarrow B$, automorphisme de B laissant fixe A. Le groupe de ces automorphismes sera noté $\text{Gal } B/A$ et les réductions successives fournissent des isomorphismes $\text{Gal } L/K \rightarrow \text{Gal } B/A \rightarrow \text{Gal } \bar{L}/\bar{K}$.

Soit maintenant B/A une extension galoisienne, M un BG-module et $\sigma \in \text{Gal } B/A$. σ induit $\sigma: BG \rightarrow BG$ et, par extension des scalaires via σ (ou par restriction via σ^{-1}), on peut mettre une nouvelle structure de BG-module sur M. On note σM l'ensemble M muni de cette structure et σx l'élément de σM correspondant à $x \in M$. L'action de BG sur σM est définie par : $g \sigma x = \sigma(gx)$ et $b \sigma x = \sigma(\sigma^{-1}(b)x)$. On a un isomorphisme semi-linéaire $\sigma: M \rightarrow \sigma M$ car $\sigma(bx) = \sigma(b) \sigma(x)$. (cf. [Ke, §5]).

Preuve de la proposition : On suppose d'abord que B/A est une extension galoisienne. Soit $N = \bigoplus_{\sigma \in \text{Gal}(B/A)} \sigma M$. $\text{Gal } B/A$ agit par automorphismes semi-linéaires sur N via $\sigma: \tau M \rightarrow \sigma(\tau M) \cong (\sigma\tau)M$. Soit $M_0 = \{ \sum_{\sigma} \sigma x \mid x \in M \}$ le sous-module diagonal. M_0 est un sous-AG-module de N et $M \cong M_0$ comme AG-module par $x \mapsto \sum_{\sigma} \sigma x$. Alors $B \otimes_A M_0 \cong N$. En effet : Soit $h: B \otimes_A M_0 \rightarrow N$. h est BG-linéaire.

$$b \otimes x \mapsto bx$$

Si $B = A[z]$ et si B est de degré n sur A , alors $1, z, z^2, \dots, z^{n-1}$ est une A -base de B . Tout élément de $B \otimes_A M_0$ s'écrit $\sum_{i=0}^{n-1} z^i \otimes x_i$, $x_i \in M_0$. Montrons que h est injective. Si $\sum_{i=0}^{n-1} z^i x_i = 0$, alors $0 = \sigma(\sum_{i=0}^{n-1} z^i x_i) = \sum_{i=0}^{n-1} \sigma(z^i) x_i$ car $\sigma(x_i) = x_i$ vu que $x_i \in M_0$. Si $\text{Gal } B/A = \{\sigma_0, \dots, \sigma_{n-1}\}$, on considère la matrice $(\sigma_j(z^i)) \in M_n(B)$. Par réduction modulo τ , on a par un calcul classique de discriminant : $\det(\bar{\sigma}_j(\bar{z}^i))^2 = \prod_{i < j} (\sigma_j(\bar{z}) - \sigma_i(\bar{z}))^2 = \prod_{i \neq j} (\sigma_j(\bar{z}) - \sigma_i(\bar{z})) = N_{\bar{L}/\bar{K}} \bar{f}'(\bar{z}) \neq 0$ où $\bar{f}$ est le polynôme minimal de z sur $\bar{K}$ et où $N_{\bar{L}/\bar{K}}$ est la norme de l'extension $\bar{L}/\bar{K}$. Ainsi $\det(\sigma_j(z^i))$ est inversible car inversible modulo τ et donc $(\sigma_j(z^i))$ est inversible. Il résulte alors du système de n équations $\sum_{i=0}^{n-1} \sigma_j(z^i) x_i = 0$ que $x_i = 0$ pour tout i . Donc h est injective.

Maintenant, comme A -modules, on a $M \cong M_0$. $B \otimes_A M_0 \cong M^n$ et $N = \bigoplus_{\sigma} \sigma M \cong M^n$. M^n étant artinien, h doit être un isomorphisme.

Finalement, M est facteur direct dans $N \cong B \otimes_A M_0$, par construction même de N .

Si maintenant B/A n'est pas galoisienne, soit C la clôture galoisienne de B . Si $\bar{L} = B/\pi B$ et $\bar{K} = A/\pi A$, C est définie comme l'unique extension non ramifiée de A d'extension résiduelle $\bar{E}/\bar{K}$ où $\bar{E}$ est la clôture galoisienne de $\bar{L}$.

Soit $p : B \otimes_A M \rightarrow M$, M étant considéré comme AG -module dans le membre de gauche. p est BG -linéaire et surjective. Etendons les scalaires à C :

$1 \otimes p : C \otimes_A M \rightarrow C \otimes_B M$ est la composée de l'isomorphisme induit par $1 : M \xrightarrow{\sim} M_0$, de l'isomorphisme $h : C \otimes_A M_0 \rightarrow N = \bigoplus_{\sigma} \sigma(C \otimes_B M)$ et de la projection $q : N \rightarrow C \otimes_B M$. En effet $qh(b \otimes x) = qh(b \otimes \sum_{\sigma} \sigma x) = q(b \cdot \sum_{\sigma} \sigma x) = b \cdot x$. Ainsi $1 \otimes p$ est scindée. Si $Q = \text{Ker } p$, on a $(C \otimes_B Q) \oplus (C \otimes_B M) \cong C \otimes_B (B \otimes_A M)$. Par la proposition 2.6., $Q \oplus M \cong B \otimes_A M$. $\square$

§3 Modules relativement projectifs.

Soient A un anneau commutatif, G un groupe et H un sous-groupe de G . Si M est un AH -module à gauche, on définit le module induit de M (de H à G) comme étant $AG \otimes_{AH} M$. C'est un AG -module à gauche via la structure de AG -module à gauche de AG . On définit de même le module coinduit de M comme étant $\text{Hom}_{AH}(AG, M)$. C'est un AG -module à gauche via la structure de AG -module à droite de AG .

Un AG-module est dit projectif relativement à H (ou (G,H)-projectif lorsqu'il n'y a pas de confusion possible concernant les scalaires) s'il est facteur direct d'un induit de H à G. Un AG-module est dit injectif relativement à H (ou (G,H)-injectif) s'il est facteur direct d'un coinduit de H à G. Lorsque $H = 1$, on dit plus simplement relativement projectif et relativement injectif. Rappelons le résultat suivant :

Proposition 2.8 : Les conditions suivantes sont équivalentes :

(i) M est (G,H)-projectif.

(ii) Si
$$\begin{array}{ccc} & M & \\ \downarrow f & & \\ N & \xrightarrow{p} Q \rightarrow 0 \end{array}$$
 est un diagramme d'applications AG-linéaires

et s'il existe $f_* : M \rightarrow N$ AH-linéaire avec $p \circ f_* = f$, alors il existe $f_{**} : M \rightarrow N$ AG-linéaire avec $p \circ f_{**} = f$.

(iii) Si une application AG-linéaire surjective $p : N \rightarrow M$ admet une section AH-linéaire, alors elle admet une section AG-linéaire.

(iv) M est facteur direct dans $AG \otimes_{AH} M_0$, où $M_0 = M$ considéré comme AH-module.

(v) $\text{res} : \text{Ext}_{AG}^1(M, N) \rightarrow \text{Ext}_{AH}^1(M, N)$ est injective pour tout AG-module N.

(vi) $\text{res} : \text{Ext}_{AG}^n(M, N) \rightarrow \text{Ext}_{AH}^n(M, N)$ est injective pour tout AG-module N et pour tout $n \geq 0$.

Preuve : (i) $\Rightarrow$ (ii) On peut supposer M induit : $M = AG \otimes_{AH} L$. On définit alors : $f_{**}(g \otimes x) = g f_*(1 \otimes x)$, $x \in L$, et on vérifie que f_{**} est AG-linéaire et que $p \circ f_{**} = f$.

(ii) $\Rightarrow$ (iii) C'est immédiat en prenant $Q = M$ et $f = 1_M$.

(iii) $\Rightarrow$ (iv) $p : AG \otimes_{AH} M_0 \rightarrow M$ est AG-linéaire et admet si $M \rightarrow AG \otimes_{AH} M_0$

$$g \otimes x \mapsto gx \qquad x \mapsto 1 \otimes x$$

comme section AH-linéaire. On applique alors (iii).

(iv) $\Rightarrow$ (i) trivial

(ii) $\Rightarrow$ (v) On plonge N dans un AG-module injectif I, avec quotient Q

$$\begin{array}{ccccc} \text{Hom}_{AG}(M, I) & \xrightarrow{\alpha} & \text{Hom}_{AG}(M, Q) & \xrightarrow{\beta} & \text{Ext}_{AG}^1(M, N) \rightarrow 0 \\ \downarrow \text{res} & & \downarrow \text{res} & & \downarrow \text{res} \\ \text{Hom}_{AH}(M, I) & \xrightarrow{\beta} & \text{Hom}_{AH}(M, Q) & \rightarrow & \text{Ext}_{AH}^1(M, N) \end{array}$$

Si $x \in \text{Ext}_{AG}^1(M, N)$ est tel que $\text{res } x = 0$, soit $f : M \rightarrow Q$ tel que $\beta f = x$. Alors $\text{res } f \in \text{Im } \beta$ et par (ii), $f \in \text{Im } \alpha$. Donc $x = \beta f = 0$.

(v) $\Rightarrow$ (vi) On plonge N dans un AG-module injectif I , avec quotient Q . I est aussi injectif comme AH-module par le lemme 2.10 qui suit.

$$\begin{array}{ccccc} 0 \rightarrow \text{Ext}_{AG}^n(M, Q) & \xrightarrow{\sim} & \text{Ext}_{AG}^{n+1}(M, N) & \rightarrow & 0 \\ \downarrow \text{res} & & \downarrow \text{res} & & \\ 0 \rightarrow \text{Ext}_{AH}^n(M, Q) & \xrightarrow{\sim} & \text{Ext}_{AH}^{n+1}(M, N) & \rightarrow & 0 \end{array}$$

Le résultat s'ensuit par induction sur $n \geq 1$. Il est toujours vrai pour $n = 0$.

(vi) $\Rightarrow$ (ii) Dans un diagramme (ii), on pose $K = \text{Ker } p$ et on a :

$$\begin{array}{ccccc} \text{Hom}_{AG}(M, N) & \xrightarrow{\alpha} & \text{Hom}_{AG}(M, Q) & \xrightarrow{\beta} & \text{Ext}_{AG}^1(M, K) \\ \downarrow \text{res} & & \downarrow \text{res} & & \downarrow \text{res} \\ \text{Hom}_{AH}(M, N) & \xrightarrow{\beta} & \text{Hom}_{AH}(M, Q) & \xrightarrow{\beta} & \text{Ext}_{AH}^1(M, K) \end{array}$$

Par hypothèse $\text{res } f = \beta(f_*)$. Donc $\text{res } \beta f = \beta \text{res } f = 0$. Par (vi), $\beta f = 0$. Ainsi $f \in \text{Im } \alpha$, i.e. $f = \alpha(f_*)$. $\square$

Dualement on a aussi :

Proposition 2.9 : Les conditions suivantes sont équivalentes :

(i) M est (G,H)-injectif.

(ii) Si $0 \rightarrow Q \xrightarrow{p} N$ est un diagramme d'applications AG-linéaires et s'il

$$\begin{array}{c} \downarrow f \\ M \end{array}$$

existe $f_* : N \rightarrow M$ AH-linéaire avec $f_* \bullet p = f$, alors il existe $f_{**} : N \rightarrow M$ AG-linéaire avec $f_{**} \bullet p = f$.

(iii) Si une application AG-linéaire injective $p : M \rightarrow N$ admet une rétraction AH-linéaire, alors elle admet une rétraction AG-linéaire.

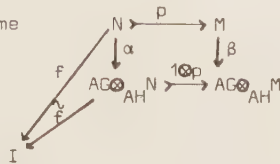
(iv) M est facteur direct dans $\text{Hom}_{AH}(AG, M_0)$ où $M_0 = M$ considéré comme AH-module.

(v) $\text{res} : \text{Ext}_{AG}^1(N, M) \rightarrow \text{Ext}_{AH}^1(N, M)$ est injective pour tout AG-module N .

(vi) $\text{res} : \text{Ext}_{AG}^n(N, M) \rightarrow \text{Ext}_{AH}^n(N, M)$ est injective pour tout AG-module N et pour tout $n \geq 0$. $\square$

Lemme 2.10 : Un AG-module injectif (respectivement projectif) est aussi injectif (respectivement projectif) considéré comme AH-module.

Preuve : Si I est AG-injectif et si $0 \rightarrow N \xrightarrow{p} M$ est un diagramme d'applications AH-linéaires, on considère le diagramme



où $\tilde{f}$ est l'unique homomorphisme AG-linéaire tel que $\tilde{f}\alpha = f$.

I étant AG-injectif, il existe $\tilde{f}_* : AG \otimes_{AH} M \rightarrow I$ tel que $\tilde{f}_*(1 \otimes p) = \tilde{f}$.

On pose $f_* = \tilde{f}_* \beta : M \rightarrow I$ et on a $f_* p = f$. Ainsi I est AH-injectif. $\square$

Il résulte de ce qui précède que, pour un AG-module M, on a :

M est AG-projectif $\iff$ M est AH-injectif et (G,H)-projectif

M est AG-injectif $\iff$ M est AH-injectif et (G,H)-injectif.

Proposition 2.11 : Si l'indice de H dans G est fini, les modules induit et coInduit coïncident.

Preuve : On définit $\phi : AG \otimes_{AH} M \rightarrow \text{Hom}_{AH}(AG, M)$ par $\phi(g_i \otimes x)(g^{-1}) = \delta_{ij} x$ où les g_i sont un système de représentants des classes à gauche de G modulo H. Les g_i forment une base de AG comme AH-module à gauche. Donc ϕ est bien définie et on voit facilement qu'elle est AG-linéaire et injective. Comme AH-modules, $AG \otimes_{AH} M \cong \bigoplus_i M$, $\text{Hom}_{AH}(AG, M) \cong \prod_i M$, et ϕ n'est autre que l'inclusion canonique $\bigoplus_i M \hookrightarrow \prod_i M$, qui est un isomorphisme lorsque l'indice de H dans G est fini. $\square$

Proposition 2.12 : Si $[G:H]$ est fini, les conditions suivantes sont équivalentes :

(i) M est (G,H)-projectif (ii) M est (G,H)-injectif

(iii) $\exists \psi \in \text{End}_{AH} M$ tel que $\sum_{i=1}^{[G:H]} g_i \psi g_i^{-1} = 1_M$ (les g_i étant un système de représentants des classes à gauche modulo H).

Preuve : (i) $\Leftrightarrow$ (ii) résulte de la proposition 2.11.

(ii) $\Rightarrow$ (iii) $M \xrightarrow{1} AG \otimes_{AH} M$ admet $AG \otimes_{AH} M \rightarrow M$ comme

$$x \mapsto \sum_1 g_i \otimes g_i^{-1} x \quad g \otimes x \mapsto \begin{cases} 0 & g \notin H \\ g x & g \in H \end{cases}$$

rétraction AH-linéaire. Il existe donc une rétraction p AG-linéaire :

$1_M = p_1$. Alors $x = p \left(\sum_1 g_i \otimes g_i^{-1} x \right) = \sum_1 g_i p a g_i^{-1} x$ où a est l'in-

clusion AH-linéaire $\alpha : M \rightarrow AG \otimes_{AH} M$. $\psi = p a$ répond alors à la question.

$$x \mapsto 1 \otimes x$$

(iii) $\Rightarrow$ (i) Si ψ existe, soit $\psi^* : AG \otimes_{AH} M \rightarrow M$. ψ^* est AG-linéaire.

$$g \otimes x \mapsto g \psi^*(x)$$

Alors ψ^* est une rétraction de $1 : \psi^* i x = \psi^* \sum_1 g_i \otimes g_i^{-1} x =$

$$= \sum_1 g_i \psi g_i^{-1} x = x. \text{ Donc } M \text{ est facteur direct dans } AG \otimes_{AH} M. \quad \square$$

Proposition 2.13 : Soient A un anneau court, G un groupe fini et M un AG-module. M est projectif si et seulement si M est injectif.

Preuve : En vertu des propositions 1.1 et 2.12, on a :

M est AG-projectif $\Leftrightarrow M$ est A-projectif et $(G, 1)$ -projectif $\Leftrightarrow M$ est A-injectif et $(G, 1)$ -injectif $\Leftrightarrow M$ est AG-injectif. $\square$

Proposition 2.14 : (Maschke). Soient A un anneau commutatif local de corps résiduel K de caractéristique p , G un groupe fini et G_p un p -sous-groupe de Sylow de G . Alors tout AG-module est (G, G_p) -projectif. (Si $p = o$, on convient que $G_p = 1$).

Preuve : $m = [G, G_p]$ est premier à p , donc inversible dans A . Si M est un AG-module, l'endomorphisme ψ de multiplication par m^{-1} est certainement AG-linéaire. $\sum_{i=1}^m g_i \psi g_i^{-1} = \sum_{i=1}^m \psi = 1_M$. Par la proposition 2.12, M est (G, G_p) -projectif. $\square$

Ce genre de résultat s'énonce aisément dans les groupes Ext :

Proposition 2.15 : Soient A un anneau commutatif, G un groupe, H un sous-groupe d'indice fini, M et N deux AG-modules. Si K est le noyau de res :

$$\text{Ext}_{AG}^n(M, N) \rightarrow \text{Ext}_{AH}^n(M, N), \text{ alors } [G : H] \cdot K = 0 \quad (n \geq 1)$$

Preuve : On peut supposer $n = 1$ car le résultat général en découle par décalage comme dans la proposition 2.8.

Soit $0 \rightarrow R \xrightarrow{\alpha} L \rightarrow M \rightarrow 0$ une présentation de M .

$$\begin{array}{ccccc} \text{Hom}_{AG}(L, N) & \xrightarrow{\alpha^*} & \text{Hom}_{AG}(R, N) & \xrightarrow{\partial} & \text{Ext}_{AG}^n(M, N) \rightarrow 0 \\ \downarrow \text{res} & & \downarrow \text{res} & & \downarrow \text{res} \\ \text{Hom}_{AH}(L, N) & \xrightarrow{\alpha^*} & \text{Hom}_{AH}(R, N) & \xrightarrow{\partial} & \text{Ext}_{AH}^n(M, N) \rightarrow 0 \end{array}$$

Soit $x \in K$ et $f: R \rightarrow N$ tel que $\partial f = x$. $\partial \text{res} f = \text{res} \partial f = \text{res} x = 0$

Donc $\text{res} f$ se relève en $h: L \rightarrow N$ AH -linéaire : $h\alpha = f$. Soient $g_1, \dots, g_n$ un système de représentants des classes à gauche de G modulo H et $\hat{h} = \sum_{i=1}^n g_i h g_i^{-1}$. $\hat{h} \in \text{Hom}_{AG}(L, N)$ et $\alpha^*(\hat{h}) = \hat{h}\alpha = \sum_{i=1}^n g_i h g_i^{-1} \alpha = \sum_{i=1}^n g_i f g_i^{-1} = mf$. Donc $mf \in \text{Im} \alpha^*$ et $mx = \partial mf = 0$. $\square$

Si $[\bar{G} : \bar{H}]$ est inversible dans A , alors $K = 0$ et res est donc injective. Cela signifie que M est relativement projectif et on retrouve le théorème de Maschke.

Corollaire : Si G est fini et si M est A -projectif, alors $|G| \cdot \text{Ext}_{AG}^n(M, N) = 0$ pour tout AG -module N , et pour $n \geq 1$.

Preuve : On prend $H = 1$ dans la proposition précédente. Comme M est A -projectif, $\text{Ext}_{AG}^n(M, N) = 0$ et donc $K = \text{Ext}_{AG}^n(M, N)$. $\square$

Ainsi si G est fini, si M est un AG -module A -projectif et si K est le noyau de la restriction $\text{res} : \text{Ext}_{AG}^n(M, N) \rightarrow \text{Ext}_{AH}^n(M, N)$, alors $|H| \cdot \text{Ext}_{AG}^n(M, N) \subset K$. En désignant, pour k un entier, par m_k l'endomorphisme de multiplication par k , on a les inclusions $\text{Im } m_k|_H \subset K \subset \text{Ker } m_k|_{[\bar{G} : \bar{H}]}$.

On n'a pas en général d'égalités. Si par exemple A est de caractéristique p , G un groupe d'ordre divisible par p^2 et H un sous-groupe d'ordre p , on a $\text{Im } m_p|_H = 0$ et $\text{Ker } m_p|_{[\bar{G} : \bar{H}]} = \text{Ext}_{AG}^n(M, N)$ tout entier, car p annule tous les groupes Ext . Si M est (G, H) -projectif sans être projectif, $K = 0$ donc $K \subsetneq \text{Ker } m_p|_{[\bar{G} : \bar{H}]}$ pour au moins un N . Sinon $\text{Im } m_p|_H = 0 \subsetneq K$ pour au moins un N .

Si A est un anneau local, le corollaire précédent s'énonce de la manière suivante :

Proposition 2.16 : Soient A un anneau local de corps résiduel de caractéristique p , G un groupe fini d'ordre $p^t \cdot m$, où $(p, m) = 1$, et M un AG -module A -libre. Pour tout AG -module N , on a $p^t \cdot \text{Ext}_{AG}^n(M, N) = 0$, $n \geq 1$.

Preuve : On a $p^t m \cdot \text{Ext}_{AG}^n(M, N) = 0$ par le corollaire précédent. Comme m est inversible dans A , le résultat s'ensuit. $\square$

§4 Questions de relèvement.

Soient A un anneau court d'uniformisante π , G un groupe fini et M, N deux AG -modules A -libres. Deux questions fondamentales se posent pour l'étude des AG -modules.

1) Si $M/\pi M \cong N/\pi N$, est-ce que $M \cong N$?

2) Si M est indécomposable, est-ce que $M/\pi M$ l'est aussi ?

On verra que les réponses à ces questions sont affirmatives dans le cas où la caractéristique du corps résiduel $K = A/\pi A$ est première à l'ordre du groupe, mais négatives dans le cas général. Ces questions sont liées à l'inversibilité de l'ordre du groupe dans A . Plus précisément, c'est la valuation π -adique s de $|G|$ qui joue un rôle fondamental. s est défini par $|G| = \pi^s u$, u étant inversible dans A .

Si K est de caractéristique nulle, s est toujours nul. Sinon, A est un p -anneau court, et si $pA = \pi^e A$, alors $s = te$, où t est la valuation p -adique de $|G|$: $|G| = p^t m$, $(p, m) = 1$. La proposition 2.16 s'énonce encore : $\pi^s \text{Ext}_{AG}^n(M, N) = 0$.

Dans l'optique des 2 questions posées, on a le résultat général suivant :

Théorème 2.17 : Soient A un anneau court de longueur r et d'uniformisante π , G un groupe fini, s la valuation π -adique de $|G|$ et M, N deux AG -modules A -libres. On suppose $r \geq 2s + 1$.

(1) Pour tout $f : M/\pi^{s+1}M \rightarrow N/\pi^{s+1}N$, il existe $g : M/\pi^{r-s}M \rightarrow N/\pi^{r-s}N$ tel que $\bar{g} = \bar{f}$ (une barre désignant la réduction modulo π)

(2) $M/\pi^{s+1}M \cong N/\pi^{s+1}N \iff M/\pi^{r-s}M \cong N/\pi^{r-s}N$

(3) $M/\pi^{s+1}M$ est indécomposable si et seulement si $M/\pi^{r-s}M$ l'est.

Il est clair que l'énoncé (1) n'a de l'intérêt que si $r-s \geq s+1$. Ceci explique la condition $r \geq 2s+1$. Comme annoncé, ces résultats donnent des réponses affirmatives aux questions posées lorsque $s = 0$. Pour $s = 1$, le point

(2) affirme que si $M/\tau^2 M = N/\tau^2 N$, alors $M/\pi^{r-1} M \cong N/\pi^{r-1} N$. Dans le cas du groupe cyclique d'ordre p et d'un anneau A non ramifié, ce qui implique $s = 1$, on verra qu'on a un résultat plus fort : $M/\tau M \cong N/\tau N \Rightarrow M/\pi^{r-1} M \cong N/\pi^{r-1} N$.

Question : Dans le cas général, a-t-on aussi le résultat plus fort :

$$M/\pi M \cong N/\pi M \Rightarrow M/\pi^{-s} M \cong N/\pi^{-s} M ?$$

Preuve du théorème :

$$\begin{array}{ccccc} (1) & \text{Les 2 suites exactes } 0 \rightarrow \pi^{s+1} N \rightarrow N \rightarrow N/\pi^{s+1} N \rightarrow 0 \text{ et} \\ & 0 \rightarrow \pi^{s+1} N \rightarrow \pi^s N \rightarrow \pi^s N / \pi^{s+1} N \text{ fournissent le diagramme commutatif :} \\ \text{Hom}(M, N) & \rightarrow \text{Hom}(M, N/\pi^{s+1} N) & \xrightarrow{\cong} & \text{Ext}(M, \pi^{s+1} N) \\ \downarrow \cdot \tau^s & \downarrow \cdot \tau^s & & \downarrow \cdot \pi^s = 0 \\ \text{Hom}(M, \pi^s N) & \rightarrow \text{Hom}(M, \pi^s N / \pi^{s+1} N) & \xrightarrow{\cong} & \text{Ext}(M, \pi^{s+1} N) \end{array}$$

Comme τ^s annule $\text{Ext}(M, \pi^{s+1} N)$, si $f_0 \in \text{Hom}(M, N/\pi^{s+1} N)$, alors $\pi^s f_0$ se relève en un homomorphisme $h : M \rightarrow \pi^s N$.

$$\begin{array}{ccccc} \text{La multiplication par } \tau^{-s} \text{ induit des isomorphismes (corollaire de la proposition 1.1) :} & \text{Hom}(M, \pi^s N) & \rightarrow & \text{Hom}(M, \pi^s N / \pi^{s+1} N) & \rightarrow & \text{Ext}(M, \pi^{s+1} N) \\ \uparrow \cong & \uparrow \cong & & \uparrow \cong & & \\ \text{Hom}(M, N/\pi^{r-s} N) & \rightarrow & \text{Hom}(M, N/\tau N) & \rightarrow & \text{Ext}(M, N/\pi^{r-s} N) \end{array}$$

Par l'inverse de ces isomorphismes, $\pi^s f_0$ est envoyé sur $\tilde{f}_0 : M \rightarrow N/\tau N$, h sur $g_0 : M \rightarrow N/\pi^{r-s} N$ et g_0 est un relèvement de $\tilde{f}_0$. De plus $\tilde{f}_0$ n'est autre que la composée de f_0 et de l'homomorphisme canonique $N/\pi^{s+1} N \rightarrow N/\tau N$.

En effet le diagramme suivant est commutatif :

$$\begin{array}{ccc} N/\pi^{s+1} N & \xrightarrow{\cdot \pi^s} & \pi^s N / \pi^{s+1} N \\ \downarrow & \nearrow \cdot \tau^s \cong & \\ N/\tau N & & \end{array}$$

Si maintenant on se donne $f : M/\pi^{s+1} M \rightarrow N/\pi^{s+1} N$, on obtient, en faisant précéder f de l'homomorphisme canonique $M \rightarrow M/\pi^{s+1} M$, un homomorphisme f_0 et on vient de montrer que $\tilde{f}_0 : M \rightarrow N/\tau N$ se relève en $g_0 : M \rightarrow N/\pi^{r-s} N$. Mais $\tilde{f}_0$ se factorise en $M \rightarrow M/\tau M \xrightarrow{\tilde{f}} N/\tau N$ et g_0 en $M \rightarrow M/\pi^{r-s} M \xrightarrow{g} N/\pi^{r-s} N$. La réduction modulo π de g n'est alors autre que $\tilde{f}$ comme le montre le diagramme suivant :

$$\begin{array}{ccccc}
 & & f_0 & & \\
 & \nearrow & & \searrow & \\
 M & \longrightarrow & M/\pi^{s+1}M & \xrightarrow{f} & N/\pi^{s+1}N \\
 \parallel & & \downarrow & & \downarrow \\
 M & \longrightarrow & M/\pi M & \xrightarrow{\bar{f}} & N/\pi N \\
 \parallel & \nearrow & & \nwarrow & \\
 M & \xrightarrow{g_0} & M/\pi^{r-s}M & \xrightarrow{g} & N/\pi^{r-s}N
 \end{array}$$

(2) Si f est l'isomorphisme $M/\pi^{s+1}M \rightarrow N/\pi^{s+1}N$, alors $\bar{f} : M/\pi M \rightarrow N/\pi N$ se relève en $g : M/\pi^{r-s}M \rightarrow N/\pi^{r-s}N$ par la partie (1). Comme $\bar{f}$ est un isomorphisme, g l'est aussi par le lemme de Nakayama et le fait que N est A -libre.

La réciproque est évidente par réduction modulo π^{s+1} compte tenu du fait que $r - s \geq s + 1$.

(3) Si $M/\pi^{s+1}M$ est décomposable, il existe un idempotent différent de l'identité $e \in \text{End}(M/\pi^{s+1}M)$. Par (1), l'idempotent $\bar{e} \in \text{End}(M/\pi M)$ se relève en un endomorphisme g de $M/\pi^{r-s}M$. Par la propriété classique de relèvement des idempotents, on peut choisir g idempotent (cf. [CR, 577]). Ainsi $M/\pi^{r-s}M$ est décomposable.

La réciproque est évidente par réduction modulo π^{s+1} . $\square$

Si A est un quotient d'un anneau de valuation discrète D (thm. 1.15), une autre question qui se pose est le lien entre les représentations sur A et sur D . Le théorème suivant dû à Maranda (cf. [CR, §76]), est tout à fait analogue au théorème 2.17 et garantit une bonne correspondance lorsque la longueur de A est supérieure à la valuation π -adique de $|G|$.

Théorème 2.18 : Soient D un anneau de valuation discrète d'uniformisante π , G un groupe fini, s la valuation π -adique de $|G|$, M et N deux DG -modules D -libres.

(1) Pour tout $f : M/\pi^{s+1}M \rightarrow N/\pi^{s+1}N$, il existe $g : M \rightarrow N$ tel que $\bar{g} = \bar{f} : M/\pi M \rightarrow N/\pi N$.

(2) $M/\pi^{s+1}M \overset{\sim}{=} N/\pi^{s+1}N \iff M \overset{\sim}{=} N$.

(3) Si D est complet, $M/\pi^{s+1}M$ est indécomposable $\iff M$ est indécomposable.

Preuve : Elle est presque en tout point la même que celle du théorème 2.17.

(1) On considère comme avant les deux suites exactes

$$0 \rightarrow \pi^{s+1}N \rightarrow N \rightarrow N/\pi^{s+1}N \rightarrow 0 \quad \text{et} \quad 0 \rightarrow \pi^{s+1}N \rightarrow \pi^s N \rightarrow \pi^s N / \pi^{s+1}N \rightarrow 0$$

et les suites d'Ext associées. D étant intègre, la multiplication par π^s dans N est injective. Par conséquent les isomorphismes induits par la multiplication par π^s dans le théorème précédent sont à remplacer ici par les isomorphismes suivants :

$$\begin{array}{ccccccc} 0 & \rightarrow & \pi^{s+1}N & \rightarrow & \pi^s N & \rightarrow & \pi^s N / \pi^{s+1}N \rightarrow 0 \\ & & \cdot \pi \uparrow \cong & & \cdot \pi \uparrow \cong & & \cdot \pi \uparrow \cong \\ 0 & \rightarrow & \pi N & \rightarrow & N & \rightarrow & N / \pi N \rightarrow 0 \end{array}$$

Le reste de la démonstration est identique en remplaçant $M/\pi^{r-s}M$ par M et $N/\pi^{r-s}N$ par N.

(2) et (3) La preuve ne change pas, la complétion de D dans le point (3) garantissant la propriété de relèvement des idempotents. $\square$

Corollaire : Si D est complet et si $A = D/\pi^{s+1}D$, alors la réduction modulo π^{s+1} définit une injection de l'ensemble des classes d'isomorphisme de AG-modules A-libres. Cette injection préserve les modules indécomposables.

Maranda a montré que cette injection préserve aussi les modules irréductibles. (cf. [CR, §76]).

Ainsi, l'étude des représentations de groupes finis sur un anneau court "contient" celle des représentations sur un anneau de valuation discrète complet.

§5 Enveloppes injectives et couvertures projectives.

Soit R un anneau et M un R-module. Rappelons qu'une enveloppe injective de M est la donnée d'un R-module injectif I et d'un homomorphisme $f : M \rightarrow I$ qui soit une extension essentielle de M (i.e. si N est un sous-module de I et si $N \cap f(M) = 0$, alors $N = 0$). De même, une couverture projective de M est la donnée d'un R-module projectif P et d'un homomorphisme $f : P \rightarrow M$ qui soit un revêtement essentiel de M (i.e. si N est un sous-module de P et si $N + \text{Ker } f = P$, ou encore si $f(N) = M$, alors $N = P$). Une enveloppe injective de M existe toujours et est unique à isomorphisme près ([CR, §57]).

Si R est artinien, une couverture projective de M existe toujours et est unique à isomorphisme près ([Se2, §14.3]). Une enveloppe injective I de M est minimale dans le sens que, si on a $g : M \rightarrow J$ avec J injectif, alors g se factorise par $I : M \xrightarrow{f} I \xrightarrow{g} J$ et I est bien sûr facteur direct dans J . De même, une couverture projective P de M est minimale dans le sens que, si on a $g : Q \rightarrow M$ avec Q projectif, alors g se factorise par $P : Q \xrightarrow{g} P \xrightarrow{f} M$ et P est bien sûr facteur direct dans Q .

Rappelons que si A est un anneau court et si G est un groupe fini, alors AG est artinien et AG -modules projectifs et injectifs coïncident (proposition 2.13). Ainsi tout AG -module M admet une enveloppe injective I ainsi qu'une couverture projective P et tous deux sont des modules projectifs. De plus, si M est de type fini, alors P l'est aussi car il existe toujours un module projectif Q de type fini dont M est quotient. De même I est aussi de type fini comme nous allons le voir plus loin.

Si M est un AG -module (à gauche), on définit le module dual de M : $M^\bullet = \text{Hom}_A(M, A)$. C'est un AG -module à droite pour l'action : $(fa)(x) = f(ax)$, $f \in M^\bullet$, $a \in AG$, $x \in M$. On peut munir $M^\bullet$ d'une structure de AG -module à gauche à l'aide de l'involution canonique de AG définie par $g \mapsto g^{-1}$ et étendue par A -linéarité. C'est là la définition classique d'une représentation duale. Si G est abélien, il n'est plus besoin de préciser que $M^\bullet$ est un AG -module à droite et si on le voit comme module à gauche, alors cette structure ne coïncide pas avec celle obtenue à l'aide de l'involution. Dans le cas $G = C_p$, on réalisera plus tard un isomorphisme des modules avec leurs duals, ce qui explique le choix de cette définition.

On vérifie aisément que l'évaluation $M^{\bullet\bullet} \rightarrow M$ est un isomorphisme de AG -modules à gauche et que si $f : M \rightarrow N$ est AG -linéaire à gauche, alors $f^\bullet : N^\bullet \rightarrow M^\bullet$ est AG -linéaire à droite. De plus, comme A est un A -module injectif (proposition 1.1.), le foncteur $\text{Hom}_A(-, A)$ est exact, et comme il est aussi contravariant, il transforme injection en surjection (et réciproquement), module projectif en module injectif (et réciproquement). De plus, le passage au dual préserve aussi les modules simples et les modules indécomposables. Le fait qu'il préserve les modules libres est un peu moins évident. Cela découle de l'existence d'un isomorphisme de (AG, AG) -bimodules

$AG \rightarrow AG^*$, provenant d'une forme bilinéaire symétrique non dégénérée
 $\langle , \rangle : AG \times AG \rightarrow A$ satisfaisant : $\langle a, bc \rangle = \langle ab, c \rangle$. (C'est là la définition d'une A-algèbre symétrique). Cette forme est définie par $\langle a, b \rangle = f(ab)$ où $f : AG \rightarrow A$ est donné par : $f(\sum_{g \in G} a_g g) = a_1$ (coefficient de $1 \in G$). On vérifie directement que cette forme est bilinéaire symétrique et qu'elle satisfait $\langle a, bc \rangle = \langle ab, c \rangle$. Elle est non dégénérée car sa matrice par rapport à la base canonique de AG est une matrice de permutation, donc inversible.

Finalement, le passage au dual transforme enveloppe injective en couverture projective (et réciproquement). En effet, il suffit de vérifier qu'une extension essentielle devient un revêtement essentiel. Or une extension $M \rightarrow I$ est essentielle si et seulement si dans tout diagramme commutatif

$$\begin{array}{ccc} M & \rightarrow & I \\ f \downarrow & \nearrow g & \\ N & & \end{array}$$

avec f injectif, alors g est injectif, alors qu'un revêtement $P \rightarrow M$ est essentiel si et seulement si dans tout diagramme commutatif

$$\begin{array}{ccc} & N & \\ g \nearrow & \downarrow f & \\ P & \rightarrow & M \end{array}$$

avec f surjectif, alors g est surjectif. Ces deux conditions étant duales l'une de l'autre, cela démontre l'assertion.

On est ainsi en mesure de montrer que si M est de type fini, alors son enveloppe injective I l'est aussi. Soit $P \rightarrow M^*$ la couverture projective de M^* . Comme M est de type fini, M^* l'est et par conséquent P aussi. En passant au dual, on a $M \cong M^{**} \rightarrow P^*$, P^* est l'enveloppe injective de M et P^* est de type fini car P l'est. On a donc montré :

Proposition 2.19 : Tout AG -module de type fini admet une enveloppe injective de type fini ainsi qu'une couverture projective de type fini.

Rappelons que l'enveloppe injective d'une somme directe est la somme directe des enveloppes injectives. En effet, si I_1 est l'enveloppe injective de M_1 ($i = 1, 2$) et si I est l'enveloppe injective de $M_1 \oplus M_2$, alors l'inclusion $M_1 \hookrightarrow M_1 \oplus M_2 \hookrightarrow I$ se factorise par I_1 et donc I_1 est un sous-module de I (On identifie tous les modules considérés à des sous-modules de I). De même $M_2 \hookrightarrow I_2 \hookrightarrow I$. Comme $M_1 \cap M_2 = 0$, on a $(I_1 \cap I_2 \cap M_1) \cap M_2 = 0$ et donc

$I_1 \cap I_2 \cap M = 0$ car l'inclusion $M_2 \subset I_2$ est essentielle. De même $I_1 \cap I_2 = 0$ car $M_1 \subset I_1$ est essentielle. Ainsi $I_1 \oplus I_2 \subset I$ et l'inclusion $M_1 \oplus M_2 \subset I$ se factorise par $I_1 \oplus I_2$. Comme I est une enveloppe injective, $I = I_1 \oplus I_2$. De même, si P_i est la couverture projective de M_i ($i = 1, 2$), alors P_i^* est l'enveloppe injective de M_i^* . Par ce qui précède, $(P_1 \oplus P_2)^* \cong P_1^* \oplus P_2^*$ est l'enveloppe injective de $(M_1 \oplus M_2)^* \cong M_1^* \oplus M_2^*$. En passant à nouveau au dual et en utilisant l'isomorphisme de chaque module avec son bidual, on voit que $P_1 \oplus P_2$ est la couverture projective de $M_1 \oplus M_2$.

Rappelons que si M est un A -module, $M(\pi)$ désigne le sous-module de tous les éléments de M annulés par π . C'est le plus grand sous-module de M annulé par π alors que $M/\pi M$ est le plus grand quotient de M annulé par π . Le revêtement $M \rightarrow M/\pi M$ est essentiel par le lemme de Nakayama. De même l'extension $M(\pi) \rightarrow M$ est essentielle car si N est un sous-module non nul de M et si $0 \neq x \in N$, alors il existe un entier s tel que $\pi^s x = 0$ et $\pi^{s-1} x \neq 0$. $\pi^{s-1} x \in N \cap M(\pi)$, qui est donc non nul.

Proposition 2.20 : Soient M un AG-module, $K = A/\pi A$ le corps résiduel de A , $M \rightarrow I$ une extension injective de M et $P \rightarrow M$ un revêtement projectif de M .

(1) $M \rightarrow I$ est une enveloppe injective de M si et seulement si $M(\pi) \rightarrow I(\pi)$ est une enveloppe injective de $M(\pi)$ considéré comme KG-module.

(2) $P \rightarrow M$ est une couverture projective de M si et seulement si $P/\pi P \rightarrow M/\pi M$ est une couverture projective de $M/\pi M$ considéré comme KG-module.

(3) Si M est A -libre, les deux conditions de (1) sont encore équivalentes à la suivante : $M/\pi M \rightarrow I/\pi I$ est une enveloppe injective de $M/\pi M$ considéré comme KG-module.

Preuve : Remarquons d'abord que $P/\pi P$ est bien KG-projectif car $P/\pi P \cong K \otimes_A P$. De même $I(\pi)$ est KG-injectif car $I(\pi) \cong \text{Hom}_A(K, I)$. Montrons (2), la preuve de (1) étant en tout point duale.

Considérons

$$\begin{array}{ccc} P & \xrightarrow{f} & M \\ \downarrow p & & \downarrow m \\ P/\pi P & \xrightarrow{\bar{f}} & M/\pi M \end{array}$$

Il suffit de montrer que f est essentiel si et seulement si $\bar{f}$ l'est. Or on a vu que p et m le sont. Si $\bar{f}$ est essentiel et si

N est un sous-module de P tel que $f(N) = M$, alors $mf(N) = \bar{f}p(N) = M/\pi M$, et comme $\bar{f}$ puis p sont essentiels, $N = P$. Réciproquement, si f est essentiel et si $\bar{N}$ est un sous-module de $P/\pi P$ tel que $\bar{f}(\bar{N}) = M/\pi M$, on pose $N = p^{-1}(\bar{N})$ et on a $mf(N) = \bar{f}p(N) = \bar{f}(\bar{N}) = M/\pi M$. Comme m et f sont essentiels, $N = P$ et donc $\bar{N} = p(N) = P/\pi P$.

L'affirmation (3) découle du fait que, si on note $f : M \rightarrow I$, $\tilde{f}$ sa restriction à $M(\pi)$ et $\bar{f}$ sa réduction modulo π , on a un diagramme commutatif :

$$\begin{array}{ccc} M/\pi M & \xrightarrow{\bar{f}} & I/\pi I \\ \pi^{-1} \downarrow \cong & & \pi^{-1} \downarrow \cong \\ M(\pi) & \xrightarrow{\tilde{f}} & I(\pi) \end{array} \quad , \quad r \text{ étant la longueur de } A. \text{ Les multiplications par } \pi^{-r-1} \text{ sont des isomorphismes car } M \text{ et } I \text{ sont } A\text{-libres et } M(\pi) = \pi^{-r-1}M, I(\pi) = \pi^{-r-1}I. \quad \square$$

Le passage au dual se comporte aussi de manière agréable par réduction modulo π :

Proposition 2.21 : $M^*(\pi) \cong (M/\pi M)^*$ et $M^*/\pi M^* \cong M^*(\pi)$. $(M/\pi M)^* \cong M^*/\pi M^*$ si M est A -libre. De plus, si N est un KG-module, le dual de N considéré comme AG-module est isomorphe au dual de N considéré comme KG-module.

Preuve : Par passage au dual, $M \rightarrow M/\pi M$ devient $(M/\pi M)^* \rightarrow M^*$ et comme $(M/\pi M)$ est annulé par π , on a $(M/\pi M)^* \xrightarrow{f^*} M^*(\pi) \rightarrow M^*$. En reprenant le dual, on a $M^* \rightarrow (M^*(\pi))^* \xrightarrow{f^*} M/\pi M$ et comme $M/\pi M$ est le plus grand quotient de M annulé par π , f^* est un isomorphisme et donc f aussi. L'autre assertion se démontre de la même manière. Si M est A -libre, $M/\pi M \cong M(\pi)$ et donc $(M/\pi M)^* \cong M^*/\pi M^*$. Quant à la dernière affirmation, elle résulte du fait que $\text{Hom}_A(N, A) \cong \text{Hom}_A(N, \pi^{-r-1}A) \cong \text{Hom}_A(N, A/\pi A) \cong \text{Hom}_K(N, K)$. $\square$

Soit M un AG-module et soit $P \xrightarrow{f} M$ sa couverture projective. Posons $N = \text{Ker} f$. Le module N est entièrement déterminé par M à isomorphisme près. En effet, si $P \xrightarrow{f'} M$ est une autre couverture projective de M , alors il existe un isomorphisme $h : P \rightarrow P'$ rendant commutatif le diagramme :

$$\begin{array}{ccc} P & \xrightarrow{f} & M \\ h \downarrow & & \downarrow \\ P' & \xrightarrow{f'} & M \end{array} \quad //$$

Par restriction au noyau de f , h induit un isomorphisme $\text{Ker} f \xrightarrow{\sim} \text{Ker} f'$.

On appellera N le complément de M . Le complément d'une somme directe $M_1 \oplus M_2$ est la somme directe des compléments de M_1 et de M_2 . En effet, les deux suites exactes $0 \rightarrow N_1 \rightarrow P_1 \rightarrow M_1 \rightarrow 0$ et $0 \rightarrow N_2 \rightarrow P_2 \rightarrow M_2 \rightarrow 0$, où P_i est la couverture projective de M_i ($i = 1, 2$), fournissent une suite exacte

$0 \rightarrow N_1 \oplus N_2 \rightarrow P_1 \oplus P_2 \rightarrow M_1 \oplus M_2 \rightarrow 0$ et on a vu que $P_1 \oplus P_2$ est la couverture projective de $M_1 \oplus M_2$. Le complément d'un module projectif étant nul, la notion de complément est intéressante surtout pour les modules qui n'ont pas de facteur projectif dans une décomposition en somme directe de sous-modules indécomposables. Ce sont en d'autres termes les modules qui n'ont pas de sous-module projectif non nul. En effet, tout sous-module projectif P d'un module M est injectif (proposition 2.13), donc facteur direct dans M et par conséquent tout facteur indécomposable de P intervient à isomorphisme près dans une décomposition de M en somme directe d'indécomposables (Krull-Schmidt). Or un tel facteur est projectif. On dira qu'un module est sans facteur projectif s'il ne possède pas de sous-module projectif non nul.

Proposition 2.22 : Soit $0 \rightarrow N \xrightarrow{i} P \xrightarrow{f} M \rightarrow 0$ une suite exacte de AG-modules avec P projectif.

(1) P est la couverture projective de M et M est sans facteur projectif si et seulement si P est l'enveloppe injective de N et N est sans facteur projectif.

(2) Si les conditions de (1) sont réalisées, alors M est indécomposable si et seulement si N l'est.

(3) Soit E l'ensemble des classes d'isomorphisme de AG-modules sans facteur projectif. Le passage au complément induit une bijection ϕ de E sur E . L'image d'une classe d'isomorphisme de modules indécomposables en est aussi une.

Preuve : (1) On montre en fait : M est sans facteur projectif $\Leftrightarrow P$ est l'enveloppe injective de N . P étant injectif, i se factorise par l'enveloppe injective P_1 de N . P_1 est facteur direct dans P : $P = P_1 \oplus P_2$. P_2 est projectif et intersecte trivialement $i(N) = \text{Ker } f$. Donc P_2 s'injecte par f dans M . Si M est sans facteur projectif, $P_2 = 0$ et donc $P = P_1$ est l'enveloppe injective de N .

Réciproquement, si Q est un facteur projectif de M , alors $M = Q \oplus M'$ (car Q est injectif). La surjection $P \rightarrow M \rightarrow Q$ est scindée, ce qui signifie qu'il existe un sous-module projectif de P , noté encore Q , qui s'injecte par f dans M . Alors Q intersecte trivialement $\text{Ker } f = i(N)$, ce qui montre que i n'est pas essentiel.

Dualement, on montre : P est la couverture projective de $M \iff N$ est sans facteur projectif.

(2) Si M est décomposable, $M = M_1 \oplus M_2$, alors $P = P_1 \oplus P_2$ où P_i est la couverture projective de M_i ($i=1,2$). La suite exacte de la donnée se décompose alors en somme directe de deux suites exactes $0 \rightarrow N_i \rightarrow P_i \rightarrow M_i \rightarrow 0$ ($i=1,2$), ce qui montre que $N = N_1 \oplus N_2$ est décomposable. La réciproque est duale.

(3) On définit une construction duale à celle du complément : Si N est un AG-module et si $N \xrightarrow{i} P$ est son enveloppe injective, on pose $M = \text{Coker } i$. M est entièrement déterminé par N à isomorphisme près. Le passage de N à M fournit une inverse de ϕ . Le reste des affirmations découle immédiatement de (1) et (2). $\square$

Les compléments de modules nous seront utiles dans la classification des modules lorsque $G = C_p$ s. En effet, il suffira de classer la "moitié" des modules, l'autre moitié s'en déduisant par passage au complément. Lorsque $G = C_p$, on verra que le bicomplément d'un module sans facteur projectif, i.e. le complément du complément de ce module, est toujours isomorphe à ce module. C'est là une circonstance qui n'a aucune raison de se produire en général:

Proposition 2.23 : Un AG-module M sans facteur projectif est isomorphe à son bicomplément si et seulement si M admet une résolution projective périodique de période 2.

Preuve : Si M est isomorphe à son bicomplément, on a deux suites exactes $0 \rightarrow N \xrightarrow{g} P \xrightarrow{f} M \rightarrow 0$ et $0 \rightarrow M \xrightarrow{k} Q \xrightarrow{h} N \rightarrow 0$, où N est le complément de M et où P et Q sont les couvertures projectives de M et N respectivement. Ces deux suites fournissent une résolution projective périodique de période 2 de M :

$\dots \rightarrow Q \xrightarrow{gh} P \xrightarrow{kf} Q \xrightarrow{gh} P \xrightarrow{f} M \rightarrow 0$. Réciproquement, si

$\dots \rightarrow Q \xrightarrow{g} P \xrightarrow{h} Q \xrightarrow{g} P \xrightarrow{f} M \rightarrow 0$ est une résolution périodique de période 2

de M , f se factorise par la couverture projective P' de M . Alors $P = P' \oplus L$ avec L projectif et $L \subset \text{Ker } f = \text{Im } g$. L étant injectif, il est facteur direct dans $\text{Im } g$ et par conséquent $Q \cong L \oplus Q'$ et la résolution est somme directe de

$\dots \xrightarrow{g'} Q' \xrightarrow{h'} P' \xrightarrow{g'} Q' \xrightarrow{f'} P' \rightarrow M \rightarrow 0$ et de $\dots L \xrightarrow{\text{id}} L \xrightarrow{0} L \xrightarrow{\text{id}} L \rightarrow 0 \rightarrow 0$.

Ainsi, quitte à remplacer P par P' et Q par Q' , on peut supposer que $P \xrightarrow{f} M$ est une couverture projective. On a alors $\text{Ker } h = \text{Im } g = \text{Ker } f$ et $\text{Ker } g = \text{Im } h \cong P/\text{Ker } h = P/\text{Ker } f \cong M$. En posant $N = \text{Ker } h$ et en cassant la résolution, on obtient deux

suites exactes $0 \rightarrow N \rightarrow P \xrightarrow{f} M \rightarrow 0$ et $0 \rightarrow M \rightarrow Q \xrightarrow{g} N \rightarrow 0$. P étant la couverture projective de M , N est le complément de M (et N est sans facteur projectif). M étant sans facteur projectif, $Q \rightarrow N$ est une couverture projective (cf. preuve de la proposition 2.22) et donc M est le complément de N . Ceci démontre que M est isomorphe à son bicomplément. $\square$

Exemple d'un module non isomorphe à son bicomplément : On prend $A = \mathbb{Z}/9\mathbb{Z}$ ou bien n'importe quel 3-anneau court non ramifié de longueur 2. $G = S_3 = \langle a, b \mid a^3 = b^2 = 1, bab = a^2 \rangle$. $AG = P_1 \oplus P_2$ où P_1 et P_2 sont des modules indécomposables projectifs engendrés par des idempotents primitifs orthogonaux $e_1 = 5 + 5b$ et $e_2 = 5 - 5b$ respectivement. P_1 et P_2 sont des A -modules libres de rang 3, de présentations $P_1 = \langle e_1 \mid (5 - 5b)e_1 = 0 \rangle$ et $P_2 = \langle e_2 \mid (5 + 5b)e_2 = 0 \rangle$. On considère A comme AG -module avec action triviale de G . On a alors une suite exacte : $0 \xrightarrow{f_1} A \xrightarrow{g_2} P_1 \xrightarrow{f_2} P_2 \xrightarrow{g_1} P_1 \xrightarrow{h} A \rightarrow 0$ où les applications sont définies par $f_1(1) = (1 + a + a^2)e_1$, $g_2(e_1) = (a - a^2)e_2$, $f_2(e_2) = (1 + a + a^2)e_2$, $g_1(e_2) = (a - a^2)e_1$, $h(e_1) = 1$, et étendues par AG -linéarité. Compte tenu du fait que b commute à $(1 + a + a^2)$ et $b(a - a^2) = -(a - a^2)b$, on vérifie aisément que les relations définissant P_1 et P_2 sont envoyées chaque fois sur zéro, ce qui montre que tous ces homomorphismes sont bien définis. Pour $i = 1, 2$, $\text{Im} f_i$ est A -libre de rang 1, de base $(1 + a + a^2)e_i$, alors que $\text{Im} g_i$ est A -libre de rang 2 de base $\{(a - a^2)e_i, (a^2 - 1)e_i\}$. Pour vérifier l'exactitude, il suffit donc de montrer que la suite est un complexe, (car tous les modules sont artiniens et un sous-module propre d'un module artinien ne peut jamais lui être isomorphe), ce qui découle du fait que $(1 + a + a^2)(a - a^2) = 0$. P_1 et P_2 étant indécomposables, chacun est la couverture projective de n'importe lequel de ses quotients. Ainsi $\text{Ker} h$ est le complément de A et $\text{Ker} g_1$ est le bicomplément de A . $\text{Ker} g_1 \not\cong A$ car leur couverture projective, P_2 et P_1 respectivement, ne sont pas isomorphes. On le voit aussi directement en constatant que b agit trivialement sur A alors qu'il agit par changement de signe sur $\text{Ker} g_1$.

En fait A est isomorphe à son "quadri-complément" et la suite exacte ci-dessus donne naissance à une résolution projective périodique de période 4 de A . La proposition 2.23. se généralise d'ailleurs de manière évidente à des périodes quelconques.

Le fait que A admette une résolution projective périodique peut se voir aussi en tensorisant par A une résolution de $\mathbb{Z}$ comme $\mathbb{Z}G$ -module, qu'on peut choisir périodique de période 4 car la cohomologie du groupe S_3 est périodique de période 4.

CHAPITRE 3 : MODULES RELATIVEMENT PROJECTIFS ET REPRESENTATIONS NON MODULAIRES

§1 Modules projectifs. Blocs

Soient A un anneau court de longueur r et d'uniformisante π , $K = A/\pi A$ son corps résiduel et G un groupe fini. Soient $S_1, \dots, S_n$ des représentants des classes d'isomorphisme de KG -modules simples. Ce sont aussi les AG -modules simples en vertu de la proposition 2.1. Soit encore Q_j la couverture projective de S_j comme KG -module ($j=1, \dots, n$). $Q_1, \dots, Q_n$ sont des représentants des classes d'isomorphisme des KG -modules indécomposables projectifs. Ils sont les facteurs d'une décomposition de KG en somme directe de sous-modules indécomposables (chaque Q_i apparaissant éventuellement avec une certaine multiplicité) et sont en bijection avec les modules simples par réduction modulo le radical R de KG : $Q_j/RQ_j \cong S_j$. RQ_j est l'unique sous-module maximal de Q_j (cf. [CR, §54] ou [Se2, §14.3]).

Soit maintenant P_i la couverture projective de Q_i considéré comme AG -module. Comme les deux revêtements $P_j \twoheadrightarrow Q_j$ et $Q_j \twoheadrightarrow S_j$ sont essentiels, P_j est aussi la couverture projective de S_j . Par conséquent, comme ci-dessus, $P_1, \dots, P_n$ sont les AG -modules indécomposables projectifs, facteurs d'une décomposition de AG , et sont en bijection avec les simples $S_1, \dots, S_n$ par réduction modulo le radical de AG .

Proposition 3.1 : $Q_j \cong P_j/\pi P_j$ pour $j = 1, \dots, n$

Preuve : Soit R le radical de AG . RP_j est l'unique sous-module maximal de P_j , donc contient πP_j . Alors $P_j/\pi P_j$ admet S_j comme unique quotient simple. Comme $P_j/\pi P_j \cong K \otimes_A P_j$ est KG -projectif, c'est donc la couverture projective de S_j , ce qui montre que $P_j/\pi P_j \cong Q_j$. $\square$

Corollaire : La réduction modulo π définit une bijection de l'ensemble $\{P_1, \dots, P_n\}$ des classes d'isomorphismes de AG -modules indécomposables projectifs sur l'ensemble $\{Q_1, \dots, Q_n\}$ des classes d'isomorphisme de KG -modules indécomposables projectifs.

Comme P_j est projectif, il est en particulier A-projectif, c'est-à-dire A-libre. Par conséquent, tous les quotients de la filtration $P_j \supset \pi P_j \supset \pi^2 P_j \supset \dots \supset \pi^{r-1} P_j \supset 0$ sont isomorphes à Q_j et les facteurs de composition de P_j sont les mêmes que ceux de Q_j , répétés r fois.

Rappelons que si R est un anneau artinien et si $R = R_1 \times \dots \times R_m$ est la décomposition de R en produit d'anneaux indécomposables, alors les R_i sont appelés les blocs de R . Soit E l'ensemble des classes d'isomorphisme de R -modules projectifs indécomposables, et désignons par $[\bar{P}] \in E$ la classe d'un module projectif indécomposable. On considère sur E la relation suivante : $[\bar{P}] \sim [\bar{Q}]$ si P et Q ont un facteur de composition en commun. $\sim$ est réflexive et symétrique. On dit que deux modules projectifs indécomposables P et Q sont liés si $[\bar{P}]$ et $[\bar{Q}]$ sont équivalents pour la relation d'équivalence engendrée par $\sim$. L'ensemble E se décompose en réunion disjointe de classes d'équivalence : $E = E_1 \cup \dots \cup E_s$. Tout module projectif indécomposable est isomorphe à Re où e est un idempotent primitif de R . Soit alors B_i (pour $i = 1, \dots, s$) le sous-module de R engendré par les modules Re où e parcourt l'ensemble des idempotents primitifs tels que $[Re] \in E_i$. Les B_i sont les blocs de R ([CR, §55]). En particulier $s = m$.

Chaque bloc B_i se décompose comme R -module en somme directe de modules indécomposables projectifs $B_i = P_{i1} \oplus \dots \oplus P_{ik_i}$ et les $[P_{ij}]$ ($j = 1, \dots, k_i$) parcourent tout l'ensemble E (avec répétition éventuelle car il se peut que $P_{ij} \cong P_{i1}$, $j \neq 1$). On dit que P appartient au bloc B_i si $[P] \in E_i$.

Proposition 3.2 : Soit $AG = B_1 \times \dots \times B_m$ la décomposition de AG en blocs. Alors $KG = B_1/\pi B_1 \times \dots \times B_m/\pi B_m$ est la décomposition de KG en blocs.

Preuve : Clairement la décomposition $KG = \prod_{i=1}^m B_i/\pi B_i$ est une décomposition de KG en produit d'anneaux et il suffit de montrer que chaque $B_i/\pi B_i$ ne se décompose plus comme anneau, c'est-à-dire que c'est un bloc. Or si Q_1 et Q_2 sont deux KG -modules projectifs indécomposables intervenant dans une décomposition de $B_i/\pi B_i$ comme KG -module, alors $Q_1 = P_1/\pi P_1$ et $Q_2 = P_2/\pi P_2$ en vertu de la proposition 3.1. P_1 et P_2 appartiennent au bloc B_i . Ils sont donc liés au sens de la relation d'équivalence définie plus haut. Cela signifie

qu'il existe des modules projectifs indécomposables $L_1, \dots, L_k$ avec $L_1 = P_1$, $L_k = P_2$ et tels que L_j et L_{j+1} ont un facteur de composition en commun ($j = 1, \dots, k-1$). Mais comme L_j a les mêmes facteurs de composition que $L_j/\pi L_j$, $L_j/\pi L_j$ et $L_{j+1}/\pi L_{j+1}$ ont un facteur de composition en commun. Ainsi $Q_1 = L_1/\pi L_1$ et $Q_2 = L_k/\pi L_k$ sont liés ce qui montre que $B_i/-B_i$ est un bloc. $\square$

§2 Classification des modules relativement projectifs.

La proposition 3.1. montre que la connaissance des KG-modules projectifs détermine entièrement celle des AG-modules projectifs. En fait elle détermine du même coup les AG-modules relativement projectifs, comme nous allons le voir.

Proposition 3.3 : Si P est un AG-module projectif indécomposable, alors $P/\pi^i P$ est indécomposable et relativement projectif. De plus, il est projectif comme $(A/\pi^i A)G$ -module.

Preuve : $P/\pi^i P$ est $(A/\pi^i A)G$ -projectif car $P/\pi^i P \cong A/\pi^i A \otimes_A P$. De plus, il admet $P/\pi P$ comme quotient et ce dernier est un KG-module indécomposable par la proposition 3.1. Donc $P/\pi^i P$ est a fortiori indécomposable. Comme P est AG-projectif, il existe $\phi \in \text{End}_A P$ tel que $\sum_{g \in G} g \phi g^{-1} = 1$ (proposition 2.12). Par réduction modulo π^i , ϕ induit $\psi \in \text{End}_A (P/\pi^i P)$ et $\sum_{g \in G} g \psi g^{-1} = 1$, ce qui montre que $P/\pi^i P$ est relativement projectif. $\square$

Théorème 3.4 : Soient $P_1, \dots, P_n$ les AG-modules indécomposables projectifs. Les modules $P_j/\pi^i P_j$ ($1 \leq i \leq r$, $1 \leq j \leq n$) forment un système complet de AG-modules indécomposables relativement projectifs deux à deux non isomorphes.

Preuve : La proposition précédente montre que ces modules sont indécomposables et relativement projectifs. Ils sont deux à deux isomorphes car si $P_j/\pi^i P_j \cong P_1/\pi^k P_1$, on a $i = k$ car le premier est annulé par π^i exactement et le second par π^k . En réduisant modulo π , on a $P_j/\pi P_j \cong P_1/\pi P_1$. Ceci implique $j = 1$ par la proposition 3.1.

Soit maintenant N un AG-module indécomposable relativement projectif. N est facteur direct d'un induit $AG \otimes_A M$ où M est un A -module. On peut supposer M indécomposable car N l'est. Donc $M \cong A/\pi^i A$ pour un certain i par le théorème 1.2.

$AG \otimes_A^{\sim} M \cong (A/\pi^i A)G$. Les facteurs indécomposables de $(A/\pi^i A)G$ sont les $(A/\pi^i A)G$ -modules projectifs indécomposables, c'est-à-dire les $P_j/\pi^i P_j$ ($j = 1, \dots, n$). Ainsi N est l'un d'eux, ce qui montre qu'il n'y a pas d'autres AG -modules indécomposables relativement projectifs. $\square$

Corollaire 3.5. : Soit N un AG -module de type fini relativement projectif et $N = N_1 \oplus \dots \oplus N_r$ une décomposition de N comme A -module en "composantes isotypiques" comme dans le corollaire 1.3. (i.e. N_i est un $A/\pi^i A$ -module libre). Alors il existe une décomposition de N comme AG -module $N = N'_1 \oplus \dots \oplus N'_r$ avec $N'_i \cong N_i$ comme A -module.

Preuve : Dans une décomposition de N en AG -modules indécomposables, chaque facteur est relativement projectif, donc isomorphe à l'un des $P_j/\pi^i P_j$ par le théorème 3.4. On regroupe alors tous les termes isomorphes à l'un des $P_j/\pi^i P_j$, pour i fixé, en un sous-module N'_i . Comme $P_j/\pi^i P_j$ est $A/\pi^i A$ -libre, N'_i l'est aussi et on a $N = N'_1 \oplus \dots \oplus N'_r$. L'isomorphisme $N'_i \cong N_i$ résulte de l'unicité à isomorphisme près de la décomposition de N comme A -module en composantes isotypiques. $\square$

§3 Représentations non modulaires.

Si la caractéristique du corps résiduel K de A est première à l'ordre du groupe G , on dira qu'un AG -module de type fini M est une représentation non-modulaire de G . Il n'est pas nécessaire dans ce cadre de supposer que M est A -libre comme nous le ferons dans le cas modulaire. K est soit de caractéristique nulle, soit de caractéristique $p \neq 0$ auquel cas A est un p -anneau court et p ne divise pas G . Aucune hypothèse sur A n'est nécessaire alors que nous devons supposer que A est un p -anneau court non ramifié dans le cas modulaire.

Le théorème de Maschke (proposition 2.14) affirme que, dans ces circonstances, tout AG -module est relativement projectif. Ainsi la liste complète des AG -modules indécomposables est donnée par le théorème 3.4, ce qui classe entièrement les AG -modules de type fini.

Si P est un AG -module indécomposable projectif, alors $P/\pi P$ est un KG -module indécomposable projectif en vertu de la proposition 3.1, donc un KG -module simple car KG est semi-simple. Ainsi $P \supset \pi P \supset \pi^2 P \supset \dots \supset \pi^{r-1} P \supset 0$ est une suite

de Jordan-Hölder de P , et c'est même l'unique telle suite car πP est l'unique sous-module maximal de P , $\pi^2 P$ est l'unique sous-module maximal de πP (car $\pi P \cong P/\pi^{r-1}P$ et $\pi P/\pi^{r-1}P$ est l'unique sous-module maximal de $P/\pi^{r-1}P$), etc. On a donc montré :

Théorème 3.6 : Soit G un groupe fini et A un anneau court d'uniformisante π et de corps résiduel K de caractéristique première à l'ordre de G . Soient $S_1, \dots, S_n$ les différents KG-modules simples. Alors :

- (1) Pour tout $j = 1, \dots, n$, il existe un AG-module projectif P_j tel que $P_j/\pi P_j = S_j$. P_j est unique à isomorphisme près.
- (2) P_j est la couverture projective de S_j et $P_j \supset \pi P_j \supset \pi^2 P_j \supset \dots \supset \pi^{r-1} P_j \supset 0$ est l'unique suite de Jordan-Hölder de P_j .
- (3) Les modules $P_i/\pi^i P_i$ ($1 \leq i \leq r$, $1 \leq j \leq n$) forment, à isomorphisme près, un système complet de AG-modules indécomposables deux à deux non isomorphes.

Le corollaire 3.5 s'énonce alors de la même manière sans hypothèse de projectivité relative sur N . Deux autres conséquences de cette classification sont les suivantes :

Corollaire 3.7 : Un AG-module M est indécomposable si et seulement si $M/\pi M$ l'est.

On retrouve là le point (3) du théorème 2.17 (avec $s = 0$).

Corollaire 3.8 : Tout AG-module indécomposable est $A/\pi^i A$ -libre pour un certain i . Pour $A = \mathbb{Z}/p^r \mathbb{Z}$, on retrouve là le théorème 5.2.2 de [Go].

Si maintenant A est un quotient d'un anneau de valuation discrète complet D (thm 1.15), alors la classification de tous les DG-modules de type fini est aisée :

Théorème 3.9 : Soit D un anneau de valuation discrète complet d'uniformisante π et de corps résiduel K de caractéristique première à l'ordre d'un groupe G . Soient $S_1, \dots, S_n$ les différents KG-modules simples. Alors :

- (1) Pour tout $j = 1, \dots, n$, il existe un DG-module projectif P_j tel que $P_j/\pi P_j \cong S_j$. P_j est unique à isomorphisme près.
- (2) P_j est la couverture projective de S_j et $P_j \supset \pi P_j \supset \pi^2 P_j \supset \dots$ est l'unique filtration (maximale) de sous-modules de P_j .

(3) Les modules $P_j/\pi^i P_j$ ($1 \leq i \leq \infty$ en convenant que $\pi^\infty = 0$) forment, à isomorphisme près, un système complet de DG-modules indécomposables de type fini deux à deux non isomorphes. Le théorème de Krull-Schmidt est vérifié pour les DG-modules de type fini.

Preuve : (1) Comme KG est semi-simple, S_j est KG-projectif. L'existence et l'unicité de P_j n'est autre que la propriété classique de relèvement des projectifs (ou des idempotents), valable d'ailleurs aussi (et surtout !) dans le cas modulaire. Rappelons que P_j est obtenu comme limite projective des modules P_{ji} où P_{ji} est la couverture projective de S_j comme $(D/\pi^i D)G$ -module [Se 2, §14.4, prop. 42].

(2) P_j est la couverture projective de S_j car la projection $P_j \xrightarrow{p} S_j$ est essentielle en vertu du lemme de Nakayama. Si Q est un sous-module maximal de P_j (DG est noethérien car D l'est), $p(Q_j) \neq S_j$ car p est essentielle et donc $p(Q_j) = 0$ car S_j est simple. Donc $Q_j \subseteq \pi P_j$ et $Q_j = \pi P_j$ par maximalité. Ainsi πP_j est l'unique sous-module maximal de P_j , et de même $\pi^{i+1} P_j$ est l'unique sous-module maximal de $\pi^i P_j$ en vertu de l'isomorphisme $\cdot \pi^i : P_j \xrightarrow{\sim} \pi^i P_j$. Ceci démontre la seconde assertion.

(3) Si M est un DG-module de type fini, soit T la D -torsion de M . C'est un sous-DG-module de M et on a la suite exacte $0 \rightarrow T \rightarrow M \rightarrow M/T \rightarrow 0$. M/T est sans D -torsion et de type fini, donc D -libre car D est principal. Mais comme M/T est relativement projectif (proposition 2.13), M/T est DG-projectif et la suite exacte est scindée. T peut être considéré comme un $(D/\pi^r D)G$ -module pour r assez grand. Il se décompose de manière essentiellement unique en somme directe de modules de type $P_j/\pi^i P_j$ ($1 \leq i \leq r$, $1 \leq j \leq n$) en vertu du théorème 3.6.

Quant à M/T , il se décompose lui aussi de manière essentiellement unique en somme directe de modules projectifs indécomposables, à savoir les P_j . C'est là aussi un résultat classique [CR, §77], mais il se déduit dans ce cas particulier de manière immédiate du théorème 2.18 (la valuation π -adique de $|G|$ est nulle). $\square$

§4 Décomposition en blocs et extension des scalaires

A désigne toujours un anneau court de longueur r , d'uniformisante π et de corps résiduel K de caractéristique première à l'ordre de G . On démontre un analogue du lemme de Schur et du théorème de Wedderburn, ce qui permet d'établir une excellente correspondance entre AG-modules et KG-modules.

Proposition 3.10 : Soient P et Q deux AG-modules projectifs indécomposables non isomorphes.

(1) $\text{Hom}_{AG}(P, Q) = 0$.

(2) $D = \text{End}_{AG} P$ est un anneau court (non nécessairement commutatif) de longueur r et d'uniformisante π . C'est une A-algèbre A-libre de type fini.

$$D/\pi D \cong \text{End}_{KG} P/\pi P.$$

Preuve : (1) Soit $f \in \text{Hom}_{AG}(P, Q)$. $\text{Im} f$ est un sous-module de Q , donc de la forme $\pi^k Q$ pour un certain k . Si $k < r$, f induit $\bar{f} : P/\pi P \rightarrow \pi^k Q / \pi^{k+1} Q$. $\bar{f}$ est nul car c'est un homomorphisme entre deux KG-modules simples non isomorphes. Ainsi $\text{Im} f \subset \pi^{k+1} Q$ contrairement au choix de k . Donc $k = r$ et $\text{Im} f = 0$.

(2) Soit $S = P/\pi P$. La réduction modulo π induit un homomorphisme $\phi : D \rightarrow \text{End}_{KG} S$.

ϕ est surjectif car si $\bar{f} \in \text{End}_{KG} S$, il existe $f \in D$ relevant $\bar{f}$ vu que P est projectif : $P \twoheadrightarrow S$. Clairement $\pi D \subset \text{Ker} \phi$. Par ailleurs, si $f \in D$ est tel

$$\begin{array}{ccc} & P & \\ f \downarrow & & \downarrow \bar{f} \\ P & \twoheadrightarrow & S \end{array}$$

que $\pi^k f = 0$, c'est-à-dire aussi tel que $\text{Im} f \subset \pi^{r-k} P$ (car P est A-libre), alors il existe $g \in D$ avec $\pi^{r-k} g = f$. Cela résulte en effet de la projectivité de P :

$$\begin{array}{ccc} & P & \\ g \nearrow & \downarrow f & \\ P & \xrightarrow{\pi^{r-k}} & \pi^{r-k} P \end{array} \quad . \quad \text{Pour } k = r-1, \text{ cela montre que } \text{Ker} \phi \subset \pi D \text{ car si } \phi(f) = 0,$$

$\text{Im} f \subset \pi P$ et il existe $g \in D$ tel que $\pi g = f$. P étant indécomposable, D est local et par conséquent D est un anneau court d'uniformisante π et de corps résiduel (non nécessairement commutatif) $D/\pi D \cong \text{End}_{KG} S$.

Si l'on prend maintenant $k = 1$, on a $D(\pi) = \pi^{r-1} D$ ce qui montre que D est un A-module libre en vertu de la proposition 1.1. Les autres affirmations sont évidentes. $\square$

Théorème 3.11 : Soient $P_1, \dots, P_n$ les AG-modules indécomposables projectifs.
 $AG = \prod_{j=1}^n \bigoplus_{m_j} (D_j^{op})$ où $D_j = \text{End}_{AG}(P_j)$ et où m_j est le nombre de fois où P_j apparaît dans une décomposition de AG en somme directe de sous-modules indécomposables.

$$\text{De plus } KG \cong \prod_{j=1}^n \bigoplus_{m_j} [(D_j / \pi D_j)^{op}].$$

Preuve : La preuve est en tout point analogue à celle du théorème de Wedderburn.

$$AG \cong \underbrace{(P_1 \oplus \dots \oplus P_1)}_{m_1} \oplus \dots \oplus \underbrace{(P_n \oplus \dots \oplus P_n)}_{m_n}. \text{ Comme } \text{Hom}_{AG}(P_i, P_j) = 0 \text{ si } i \neq j,$$

$$\text{End}_{AG} \cong \prod_{j=1}^n \text{End}_{AG}^{m_j}(P_j \oplus \dots \oplus P_j) \cong \prod_{j=1}^n \bigoplus_{m_j} (\text{End}_{AG}^{P_j}) \cong \prod_{j=1}^n \bigoplus_{m_j} (D_j). \text{ Le résultat découle alors de l'isomorphisme d'anneaux : } \text{End}_{AG} \xrightarrow{\sim} (AG)^{op}, \text{ l'anneau opposé}$$

$$f \longmapsto f(1)$$

intervenant comme à l'accoutumée à cause du fait que AG est considéré comme AG-module à gauche.

L'affirmation concernant KG est immédiate. On peut d'ailleurs la voir comme un cas très particulier de la proposition 3.2. $\square$

Si B est une extension non ramifiée de A de corps résiduel L, alors le comportement de l'extension des scalaires de A à B des AG-modules "se lit" entièrement dans celui de l'extension des scalaires de K à L des KG-modules :

Proposition 3.12 : Soient M et N deux AG-modules indécomposables non isomorphes, $\bar{M}$ et $\bar{N}$ les KG-modules simples $\bar{M} = M/\pi M$ et $\bar{N} = N/\pi N$. Alors :

(1) $B \otimes_A M$ et $B \otimes_A N$ n'ont pas de facteur indécomposable en commun dans leur décomposition en somme directe d'indécomposables.

(2) Si $B \otimes_A M = M_1 \oplus \dots \oplus M_k$ où les M_i sont BG-indécomposables, alors $L \otimes_K \bar{M} = \bar{M}_1 \oplus \dots$ et les $\bar{M}_i$ sont LG-simples.

(3) Si $L \otimes_K \bar{M} = \bar{M}_1 \oplus \dots \oplus \bar{M}_k$ où les $\bar{M}_i$ sont LG-simples, alors il existe des BG-modules indécomposables M_i tels que $\bar{M}_i \cong M_i/\pi M_i$ et $B \otimes_A M \cong M_1 \oplus \dots \oplus M_k$.

(4) M est absolument indécomposable si et seulement si $\bar{M}$ est absolument simple.

Preuve : (2), (3) et (4) résultent immédiatement de la classification des modules (théorème 3.6 et corollaires). A noter que (4) est aussi une conséquence des propositions 2.4. et 3.10.

(1) $M \cong P/\pi^i P$ et $N \cong Q/\pi^j Q$ où P et Q sont projectifs indécomposables. Si $i \neq j$, tous les facteurs indécomposables de $B \otimes_A M$ sont $B/\pi^i B$ -libres alors que ceux de $B \otimes_A N$ sont $B/\pi^j B$ -libres et l'assertion en découle. Si $i = j$, alors $P \not\cong Q$ et donc $\bar{M} \not\cong \bar{N}$. Il est bien connu qu'alors $L \otimes_K \bar{M}$ et $L \otimes_K \bar{N}$ n'ont pas de facteur de composition en commun [Se2, §14.6]. $B \otimes_A M$ et $B \otimes_A N$ n'ont donc à fortiori pas de facteur indécomposable en commun. $\square$

Rappelons qu'un AG-module est dit irréductible s'il est A -libre et s'il ne possède pas de sous-AG-module A -libre non trivial. Dans notre cas, les AG-modules irréductibles sont exactement les AG-modules projectifs indécomposables. On a alors :

Proposition 3.13 : Les conditions suivantes sont équivalentes :

- (i) Tout AG-module irréductible est absolument irréductible.
- (ii) Tout AG-module indécomposable est absolument indécomposable.
- (iii) Tout KG-module simple est absolument simple.

Par définition, (iii) signifie que K est un corps de décomposition de G . Si ces conditions sont satisfaites, on dira que A est un anneau de décomposition du groupe G .

Preuve : (i) $\Rightarrow$ (ii) Soit $P/\pi^i P$ un AG-module indécomposable où P est projectif indécomposable. P étant irréductible, $B \otimes_A P$ est irréductible pour tout extension B de A . Alors $B \otimes_A P/\pi^i P \cong (B \otimes_A P)/\pi^i (B \otimes_A P)$ est indécomposable (corollaire 3.7).
(ii) $\Rightarrow$ (iii) résulte de la proposition 3.12 (4).

(iii) $\Rightarrow$ (i) Si P est irréductible, c'est-à-dire projectif indécomposable, P est absolument indécomposable car $P/\pi P$ est absolument simple. Pour toute extension B de A , $B \otimes_A P$ est projectif indécomposable, c'est-à-dire irréductible. $\square$

Comme il existe toujours une extension finie L de K telle que L soit corps de décomposition du groupe G , il existe aussi une extension finie B de A (extension non ramifiée de corps résiduel L) qui est anneau de décomposition de G .

Terminons par un exemple. On prend $G = C_m$ groupe cyclique d'ordre m , m étant bien sûr premier à la caractéristique de K . $AC_m \cong A[X]/(X^m-1)$. Si $X^m-1 = \prod_{j=1}^n \bar{f}_j$ est la décomposition de X^m-1 en polynômes irréductibles sur K , alors les KG-modules simples sont les modules $S_j = K[X]/(\bar{f}_j)$. Le relèvement des modules simples S_j en AG-modules projectifs indécomposables correspond ici au relèvement

de la décomposition $X^m-1 = \prod_{j=1}^n \bar{f}_j$ sur K en une décomposition $X^m-1 = \prod_{j=1}^n f_j$ sur A . Comme m est premier à la caractéristique de K , les $\bar{f}_j$ sont tous distincts et par conséquent un tel relèvement existe par le lemme de Hensel.

La décomposition $K C_m \cong \prod_{j=1}^n K[X]/(\bar{f}_j)$ se relève en $A C_m \cong \prod_{j=1}^n A[X]/(f_j)$.

Les $A C_m$ -modules $P_j = A[X]/(f_j)$ sont les projectifs indécomposables et les modules $P_j / \pi^i P_j \cong (A/\pi^i A)[X]/(f_j)$ forment l'ensemble de tous les indécomposables.

Si K contient les racines m -èmes de l'unité, les f_j , comme les $\bar{f}_j$, sont de degré $f_j = X - \omega^j$ où ω est une racine primitive m -ème de 1 dans A . Les P_j sont alors A -libres de rang 1 et par conséquent absolument indécomposables. Ainsi A est un anneau de décomposition de C_m si et seulement si A (ou K) contient les racines m -èmes de l'unité.

CHAPITRE 4 : REPRESENTATIONS MODULAIRES DE GROUPES CYCLIQUES

§1 Représentations modulaires.

Soient p un nombre premier, A un p -anneau court (i.e. p est la caractéristique du corps résiduel K de A) et G un groupe fini d'ordre divisible par p . Un AG-module de type fini M sera appelé une représentation modulaire de G . Nous ferons désormais les deux hypothèses suivantes :

1) A est un p -anneau court non-ramifié. En d'autres termes p est une uniformisante de A . Ce n'est pas une hypothèse très restrictive car on sait que pour tout corps K de caractéristique p , il existe un (et un seul) p -anneau court non ramifié de longueur donnée et de corps résiduel K (corollaire 1.16). En particulier, si $K = \mathbb{F}_p$, alors $A = \mathbb{Z}/p^r\mathbb{Z}$, ce qui permet de traiter le cas des représentations de G sur un groupe abélien fini.

2) M est un AG-module A-libre, ou encore A-projectif (proposition 1.1). Cette dernière hypothèse est courante car elle permet entre autres de mettre une structure d'anneau sur les groupes de Grothendieck, le produit tensoriel $M \otimes_A -$ étant alors un foncteur exact. Dans l'optique des représentations de G sur un groupe abélien fini, cette hypothèse est en revanche peu naturelle et il serait intéressant de pouvoir la supprimer. Mais le fait que le corollaire 3.5 soit faux pour des modules non relativement projectifs complique alors particulièrement l'étude des AG-modules en toute généralité.

Des contre-exemples au corollaire 3.5 dans le cas non relativement projectif foisonnent. En voici un assez simple : on prend $G = C_p = \langle g \mid g^p = 1 \rangle$ et A un p -anneau court non ramifié de longueur $r \geq 2$. Soit $M = M_1 \oplus M_2$ comme A -module où $M_1 \cong A/pA$ engendré par x et $M_2 \cong A$ engendré par y . On définit une action de G sur M par $gx = x$ et $gy = y + x$. Il s'agit bien d'une action de G car, comme $px = 0$, $g^p y = y$. Si M était décomposable comme AG-module, $M = M'_1 \oplus M'_2$, on aurait $M'_2 \cong A$ engendré par un élément $y' = ax + by$ comme A -module. b serait inversible sinon $p^s y' = 0$ pour un $s < r$. Alors $b^{-1}(g-1)y' = x \in M'_2$, $b^{-1}(y'-ax) = y \in M'_2$ et donc $M'_2 = M$, ce qui est absurde.

Un premier problème qui se pose est celui de la finitude du nombre des modules indécomposables (à isomorphisme près). Il résulte du théorème 3.6 qu'il y a un nombre fini de modules indécomposables dans le cas non-modulaire. En utilisant par anticipation la classification des AC_p -modules A-libres, on peut énoncer :

Théorème 4.1 : Soient A un p-anneau court non ramifié de longueur $r \geq 2$ et G un groupe fini. Alors :

Il y a un nombre fini de AG-modules de type fini indécomposables si et seulement si p ne divise pas l'ordre de G.

Plus précisément, si p divise $|G|$, il existe des AG-modules A-libres indécomposables de rang sur A arbitrairement grand.

Preuve : Compte tenu de la finitude du nombre des indécomposables, lorsque p ne divise pas $|G|$ (théorème 3.6), il suffit de montrer la 2ème assertion. Pour G cyclique d'ordre p, cela résulte immédiatement de la classification explicite des AC_p -modules A-libres que nous allons entreprendre (§6). Dans le cas général, G possède un sous-groupe H cyclique d'ordre p et on va procéder par induction de modules de n à G.

Tout d'abord, si M est un AH-module, alors M est facteur direct dans le module induit $AG \otimes_{AH} M$ considéré comme AH-module. En effet, si $\{1, g_1, \dots, g_n\}$ est un système de représentants des classes à gauche de G modulo H, $AG \otimes_{AH} M = (1 \otimes M) \oplus \bigoplus_{i=1}^n g_i \otimes M$ et $1 \otimes M \cong M$. Si maintenant M est indécomposable et A-libre de rang m, $AG \otimes_{AH} M$ possède, comme AG-module, un facteur indécomposable N, contenant un facteur isomorphe à M lorsqu'on le considère comme AH-module. Le rang de N est alors supérieur ou égal à m et comme m peut être choisi arbitrairement grand en vertu du premier cas, cela démontre (2) . $\square$

Remarques : 1) Les AG-modules indécomposables N du théorème sont tous projectifs relativement à H par construction. On a ainsi montré un résultat plus fort que (2), car si l'on sait par le théorème de Maschke que tout AG-module est (G, G_p) -projectif où G_p est un p-sous-groupe de Sylow de G, il existe néanmoins en général des modules qui sont (G, G_p) -projectifs sans être (G, H) -projectifs.

2) L'hypothèse sur la longueur r de A est nécessaire car si $r = 1$, A est un corps et il y a un nombre fini de AG-modules indécomposables si et seulement si les p -sous-groupes de Sylow de G sont cycliques [CR, §64].

(3) Dans le cas $A = \mathbb{Z}/p^r\mathbb{Z}$, on retrouve un résultat de Drobotenko et Lichtman [DL] et [GDL].

4) Si l'on veut éviter la classification complète des AC_p -modules A -libres, on peut trouver dans [HR, §5] un exemple d'une famille infinie de AC_p -modules A -libres indécomposables. L'exemple est donné pour $A = \mathbb{Z}/p^2\mathbb{Z}$ mais se généralise facilement.

§2 Les types de AC_p -modules.

Désormais A désignera un p -anneau court non ramifié de longueur $r \geq 2$ et g un générateur du groupe cyclique $G = C_p$. L'homomorphisme $\phi : A[X] \rightarrow AG$ défini par $\phi(X) = g$ induit un isomorphisme $A[X]/(X^p - 1) \xrightarrow{\sim} AG$. Tout AG-module peut être considéré comme un $A[X]$ -module annulé par $X^p - 1$, l'action de g s'identifiant à la multiplication par X . Selon nos besoins, nous utiliserons librement l'une ou l'autre de ces notations. En particulier, les polynômes seront vus souvent comme polynômes en g .

Si M est un AG-module, M/pM est un KG-module où $K = A/pA$.

Or $KG \xrightarrow{\sim} K[X]/(X^p - 1) = K[X]/(X-1)^p$ car K est de caractéristique p . $K[X]/(X-1)^p$ est un anneau court de longueur p et d'uniformisante $X-1$. Par le théorème 1.2, les modules $K[X]/(X-1)^k$, ($k=1, \dots, p$), forment un système complet de KG-modules indécomposables. Ainsi $M/pM \xrightarrow{\sim} \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$, $1 \leq k_i \leq p$.

Si tous les k_i sont égaux à k , on dira que M/pM est de type k . En d'autres termes, M/pM est de type k si c'est un $K[X]/(X-1)^k$ -module libre. Tout KG-module est donc somme directe de modules de type k , k variant entre 1 et p .

Un AG-module M sera dit de type k si M/pM est de type k . Si $G = C_p$, on verra que tout AG-module A -libre est somme directe de modules de types k mais ce résultat ne se généralise pas pour $s \geq 2$ (cf. §5).

Si Q est un diviseur unitaire (i.e. de coefficient dominant 1) de $X^{p^s} - 1$, la surjection $A[X]/(X^{p^s} - 1) \rightarrow A[X]/(Q)$ permet de considérer $A[X]/(Q)$ comme un AG-module. Ce module est A-libre de rang $k = \deg Q$. Comme $Q \equiv (X-1)^k \pmod{p}$, c'est un module de type k . Nous allons voir qu'il n'existe pas de module A-libre de type k pour n'importe quelle valeur de k et notre première tâche est d'étudier les degrés possibles des diviseurs du polynôme $X^{p^s} - 1$.

Proposition 4.2 : La plus grande puissance de $X-1$ qui divise $X^{p^s} - 1$ est $p^{s-(r-1)}$ si $r \leq s+1$ et 1 si $r \geq s+1$.

Lemme : Si x est un élément d'un anneau de caractéristique p^r et si $s \geq r-1$, alors $(x+1)^{p^s} = (x^{p^{s-(r-1)}} + 1)^{p^{r-1}}$.

Preuve : $\binom{p^r}{k} = 0 \pmod{p^r}$ si $p \nmid k$ comme on le voit facilement.

De plus $\binom{p^r}{pi} \equiv \binom{p^{r-1}}{i} \pmod{p^r}$. En effet, dans l'expression explicite de $\binom{p^r}{pi}$, les termes du numérateur de la forme p^{r-k} , pour $p \nmid k$, sont congrus à $-k \pmod{p^r}$, donc se simplifient avec les termes correspondant du dénominateur et les signes moins disparaissent car en nombre pair lorsque p est impair ou lorsque $p = 2$ et i pair. En simplifiant par p les termes restant, on obtient exactement $\binom{p^{r-1}}{i}$. Lorsque $p = 2$ et i est impair, on a par le même raisonnement $\binom{2^r}{2i} \equiv -\binom{2^{r-1}}{i} \pmod{2^r}$. Mais $-\binom{2^{r-1}}{i} \equiv \binom{2^{r-1}}{i} \pmod{2^r}$ car $-2^{r-1} \equiv 2^{r-1} \pmod{2^r}$.

On démontre alors l'égalité désirée par récurrence sur s , le cas $s = r-1$ étant trivial. $(x+1)^{p^s} = ((x+1)^{p^{s-1}})^p = (x^{p^{(s-1)-(r-1)}} + 1)^{p^r}$ par récurrence. $(x^{p^{s-r}} + 1)^{p^r} = \sum_{k=0}^{p^r} \binom{p^r}{k} x^k p^{s-r} = \sum_{i=0}^{p^{r-1}} \binom{p^{r-1}}{i} p^{i p^{s-r}} = (x^{p^{s-(r-1)}} + 1)^{p^{r-1}}$ compte tenu des deux congruences ci-dessus.

Preuve de la proposition : Si $r \leq s+1$, on a par le lemme :

$$X^{p^s} - 1 = (1 + (X-1))^{p^s} - 1 = (1 + (X-1)^{p^{s-(r-1)}})^{p^{r-1}} - 1 = p^{r-1} (X-1)^{p^{s-(r-1)}} + \binom{p^{r-1}}{2} (X-1)^{2p^{s-(r-1)}} + \dots \quad \text{et le résultat s'ensuit.}$$

Si $r \geq s+1$, alors par réduction modulo p^{s+1} , on voit que seul $X-1$ à la puissance 1 divise $X^{p^s} - 1$. $\square$

Corollaire 4.3 : Si $r \leq s$, il existe pour tout $k \leq p^{s-r+1}$ un diviseur Q de degré k de $X^{p^s} - 1$. En particulier, il existe un AG-module de type $k : A[X]/(Q)$.

Proposition 4.4 : Soit Q un diviseur unitaire de degré k de $X^{p^s}-1$, $s \geq 1$.

(1) $k \leq p^{s-1}$ ou $k \geq p^s - p^{s-1}$.

(2) Si $s = 1$, $k = 0, 1, p-1$ ou p .

Preuve : (1) Quitte à réduire modulo p^2 , on peut supposer $r=2$.

$X^{p^s}-1 = Q \cdot R$, Q étant de degré m et R de degré n . On peut supposer $m \leq n$ et il faut montrer que $m \leq p^{s-1}$. On a $m + n = p^s$ car Q et R sont unitaires. Comme

$$X^{p^s}-1 \equiv (X-1)^{p^s} \pmod{p}, \quad Q = (X-1)^m + pU \text{ et } R = (X-1)^n + pV \text{ où } U, V \in A[X].$$

$$\text{Alors : } X^{p^s}-1 = (X-1)^{p^s} + p(X-1)^m V + p(X-1)^n U \text{ car } p^2 = 0.$$

Si m était supérieur à p^{s-1} , $X^{p^s}-1$ serait divisible par une puissance de $X-1$ supérieure à p^{s-1} , contrairement à la proposition 4.2 ($r=2$).

(2) est un cas particulier de (1). $\square$

Remarque : Les diviseurs "usuels" de $X^{p^s}-1$ sont bien sûr $X-1$ et $\sum_{k=0}^{p-1} X^k$ et (2) montre que tout autre diviseur unitaire propre Q de $X^{p^s}-1$ est de même degré que l'un de ces deux. A noter qu'on n'a pas unicité de la décomposition de $X^{p^s}-1$ en facteurs irréductibles car A n'est pas intègre. En fait, si Q est de degré 1, il est de la forme $Q = X - (ap^{r-1} + 1)$, $a \in A$. Q divise $X^{p^s}-1$, car $X^{p^s}-1 = (X - ap^{r-1})^{p-1} = Q \cdot \sum_{k=0}^{p-1} (X - ap^{r-1})^k$.

Les modules $A[X]/(Q)$ correspondant donnent en fait la liste de toutes les représentations de rang 1 de C_p , chacune étant entièrement caractérisée par la classe de a dans le corps résiduel K . Nous y reviendrons (ex. 3 suivant le théorème 4.17).

Proposition 4.5 : Soit M un AG-module tel que M/pM est somme directe de modules de type k_1 , chaque k_1 étant inférieur ou égal à p^{s-1} (respectivement strictement inférieur à 2^{s-1} dans le cas $p = 2$). Alors :

$(g^{p^{s-1}} - 1)M \subset M(p)$. En particulier $(g^{p^{s-1}} - 1)M \subset p^{r-1}M$ si M est A -libre.

Preuve : Remarquons que l'hypothèse est équivalente à $(g-1)^k M \subset pM$ où k est le maximum des k_1 . Posons $N = (g^{p^{s-1}} - 1)M$. N est un sous-module de M annihilé par $\Phi(g) = \sum_{k=0}^{p-1} g^{kp^{s-1}}$ car $\Phi(g) \cdot (g^{p^{s-1}} - 1) = g^{p^s} - 1 = 0$. Ainsi N est un B -module où $B = A[X]/(\Phi(x))$. En vertu de l'exemple 1.12, B est une extension

totalelement ramifiée de A de degré $e = (p-1)p^{s-1}$ et donc $pB = (X-1)^e B$. Alors comme $(g-1)^k M \subset pM$, on a : $(g-1)^k N = (g^{p^{s-1}})(g-1)^k M \subset (g^{p^{s-1}}-1)pM = pN = (g-1)^e N \subset (g-1)^k N$, car $e = (p-1)p^{s-1} \geq p^{s-1} \geq k$. De plus l'hypothèse faite sur k implique que $k < e$. Ainsi $pN = (g-1)^k N = (g-1)^{k+1} N = \dots = (g-1)^e N = \dots = 0$ car $g-1$ est nilpotent. $\square$

Corollaire 4.6 : Si $p \neq 2$, si $G = C_p(s-1)$ et si M est un AG-module A-libre de type 1, alors $(g-1)M \subset p^{r-1}M$.

Ce résultat signifie donc qu'il suffit de supposer $(g-1)M \subset pM$ pour que $(g-1)M \subset p^{r-1}M$, ce qui sera à la base de la classification des AC_p -modules A-libres.

Proposition 4.7 : Soit Q un polynôme unitaire de degré $k \leq p^{s-1}$ de $A[X]$. ($k < 2^{s-1}$ si $p = 2$). $Q \mid (X^{p^s}-1)$ si et seulement si $Q \mid (X^{p^{s-1}}-1) \bmod p^{r-1}$.

Preuve : Soit $M = A[X]/(Q)$. Si $Q \mid (X^{p^s}-1)$, M est un AG-module A-libre de type k . Par la proposition 4.5, $(X^{p^{s-1}}-1)M \subset p^{r-1}M$ ou encore $(X^{p^{s-1}}-1)M/p^{r-1}M = 0$. Cela revient à dire que Q divise $X^{p^{s-1}}-1$ sur l'anneau $A/p^{r-1}A$. Réciproquement, si $Q \mid (X^{p^{s-1}}-1) \bmod p^{r-1}$, alors $(X^{p^{s-1}}-1)M/p^{r-1}M = 0$, donc $(X^{p^{s-1}}-1)M \subset p^{r-1}M$ et $(X^{p^{s-1}}-1)pM = 0$. En particulier $X^{p^{s-1}}$ agit trivialement sur $p^{r-1}M \subset pM$. Ainsi, $(X^{p^s}-1)M = (\sum_{k=0}^{p-1} X^{kp^{s-1}})(X^{p^{s-1}}-1)M \subset (\sum_{k=0}^{p-1} X^{kp^{s-1}})p^{r-1}M = p \cdot p^{r-1}M = 0$. Cela signifie que Q divise $X^{p^s}-1$. $\square$

La décomposition de $X^{p^s}-1$ sur $\mathbb{Z}$ est bien connue : $X^{p^s}-1 = \prod_{d \mid p^s} \phi_d$, où ϕ_d est le polynôme cyclotomique des racines d -èmes de l'unité : $\phi_1 = X-1$ et $\phi_t = \sum_{k=0}^{p-1} X^{kp^{t-1}}$, $1 \leq t \leq s$. Tout diviseur unitaire de $X^{p^s}-1$ sur $\mathbb{Z}$ est un produit de certains ϕ_d . Un tel diviseur sera appelé pour simplifier diviseur usuel de $X^{p^s}-1$. Si Q est un diviseur unitaire de $X^{p^s}-1$ de même degré qu'un diviseur usuel P , alors $Q \equiv P \bmod p$ car leur réduction mod p est un diviseur de degré k de $X^{p^s}-1 = (X-1)^{p^s}$ qui ne peut être que $(X-1)^k$ dans chaque cas. La proposition 4.4 montre que si $s = 1$, tout diviseur unitaire de X^p-1 est congru mod p à un diviseur usuel ($k=0, 1, p-1$ ou p). Ce résultat se généralise à s quelconque pour autant qu'on suppose $r \geq s+1$, ce qui supprime la possibilité qu'une puissance de $X-1$ supérieure à 1 divise $X^{p^s}-1$:

Proposition 4.8 : Si $r \geq s+1$ et si Q est un diviseur unitaire de $X^{p^s}-1$, alors Q est congru mod p à un diviseur usuel de $X^{p^s}-1$.

Preuve : On procède par récurrence sur s , le cas $s = 1$ résultant de la proposition 4.4. (on a toujours supposé $r \geq 2$ et ici $2 = s+1$). En remplaçant au besoin Q par $(X^{p^s}-1)/Q$, on peut supposer $k = \deg Q \leq p^{s-1}$ en vertu de la proposition 4.4. Par la proposition 4.7, Q divise $X^{p^{s-1}}-1$ sur l'anneau $A/p^{r-1}A$, de longueur $r-1$, à moins que $p = 2$ et $k = 2^{s-1}$. Comme $r \geq s+1$, on a $(r-1) \geq (s-1) + 1$ et la récurrence s'applique. Ainsi Q est congru mod p à un diviseur usuel P de $X^{p^{s-1}}-1$, mais P est bien sûr aussi un diviseur usuel de $X^{p^s}-1$. Reste le cas $p = 2$ et $k = 2^{s-1}$ qui est évident car Q est congru mod p à $X^{2^{s-1}}-1$ vu qu'ils sont de même degré.

Remarque : Si $r \leq s+1$, les degrés possibles k des diviseurs unitaires de $X^{p^s}-1$ peuvent être déterminés par le même argument d'induction que celui de la proposition, mais une démonstration détaillée nécessiterait un formalisme pénible. Si $r = 2$, $(X-1)^{p^{s-1}}$ divise $X^{p^s}-1$ et il y a 2 groupes de valeurs consécutives de k possibles : $0 \leq k \leq p^{s-1}$, $p^s - p^{s-1} \leq k \leq p^s$. Si $r = 3$, $(X-1)^{p^{s-2}}$ divise $X^{p^s}-1$ et il y a 4 groupes de valeurs : $0 \leq k \leq p^{s-2}$, $p^{s-1} - p^{s-2} \leq k \leq p^{s-1}$, $p^s - p^{s-1} \leq k \leq p^s - p^{s-1} + p^{s-2}$, $p^s - p^{s-2} \leq k \leq p^s$, car les valeurs $\leq p^{s-1}$ sont déterminées par récurrence par le cas $r = 2$ précédent (proposition 4.7). Dans le cas général, il y a 2^{r-1} groupes de valeurs, chacun comportant $p^{s-(r-1)+1}$ valeurs consécutives. A partir de $r = s+1$, il y a 2^s groupes de valeurs, chacun comportant 2 valeurs consécutives : $0, 1, p-1, p, p^2-p, p^2-p+1, p^2-1, p^2$, etc. Ces 2^{s+1} valeurs correspondent aux degrés des 2^{s+1} diviseurs usuels de $X^{p^s}-1$. En définitive, tout est déterminé par le premier groupe de valeurs, c'est-à-dire par la plus grande puissance de $X-1$ divisant $X^{p^s}-1$. A noter que pour $p = 2$, toutes les valeurs de 0 à p^s sont possibles.

Proposition 4.9 : Soit M un AG-module A -libre de type fini. $M/pM = \bigoplus_{i=1}^n K[\tilde{X}]/(X-1)^{k_i}$. Alors pour tout $i = 1, \dots, n$, soit $k_i \leq p^{s-1}$, soit $k_i \geq p^s - p^{s-1}$.

Preuve : 1er cas : $n=1$. $M/pM \cong K[X]/(X-1)^k$, $1 \leq k \leq p^s$. $\{1, X, X^2, \dots, X^{k-1}\}$ est une K -base de M/pM . Soit $x \in M$ ayant pour image 1 dans M/pM . Comme g agit par multiplication par X dans M/pM , $\{g^i x \mid 0 \leq i \leq k-1\}$ est une A -base de M se projetant sur la K -base de M/pM , par le lemme de Nakayama. Ainsi x engendre M comme AG-module, donc à fortiori comme $A[X]$ -module, X agissant comme g . On a alors un homomorphisme surjectif $\phi : A[X] \rightarrow M$ défini par $\phi(1) = x$. Si $g(g^{k-1}x) = \sum_{i=0}^{k-1} a_i g^i x$, alors le polynôme $Q = X^k - \sum_{i=0}^{k-1} a_i X^i$ appartient à $\text{Ker } \phi$. Ainsi ϕ induit un isomorphisme $A[X]/(Q) \cong M$ car les deux modules sont

A-libres de même rang. Comme M est un AG-module, $X^{p^s}-1$ annule M, donc Q divise $X^{p^s}-1$. Par la proposition 4.4, $k \leq p^{s+1}$ ou $k \geq p^s - p^{s-1}$.

2ème cas : n quelconque. On peut supposer que la longueur r de A est égale à 2 car M/p^2M est un $(A/p^2A)G$ -module A/p^2A -libre ayant même réduction modulo p que M.

$M/pM \cong \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$. On désigne par 1_i l'unité de $K[X]/(X-1)^{k_i}$. $\{X^s 1_i \mid 1 \leq i \leq n, 0 \leq s \leq k_i-1\}$ est une K-base de M. Soit $x_i \in M$ ayant pour image 1_i dans M/pM . $\{g^s x_i \mid 1 \leq i \leq n, 0 \leq s \leq k_i-1\}$ est une base de M. Comme $K[X]/(X-1)^{k_i}$ est invariant par l'action de g, on a :

$g(g^{k_i-1} x_i) = \sum_{j=0}^{k_i-1} a_j g^j x_i + p u_i$ où u_i est combinaison linéaire des $g^s x_i$ pour $1 \neq i$. La matrice de g dans cette base est donc de la forme :

$$g = \begin{pmatrix} (a_1) & & * \\ & \ddots & \\ * & & (a_n) \end{pmatrix} \quad \text{où} \quad a_i = \begin{pmatrix} 0 & & a_{00} \\ 1 & 0 & a_{01} \\ & \ddots & \vdots \\ & & 1 & a_{k_i-1} \end{pmatrix} \quad \text{et où les termes en dehors}$$

des blocs (a_i) sont tous multiples de p. Alors :

$$1 = g^{p^s} = \begin{pmatrix} (a_1) & & * \\ & \ddots & \\ * & & (a_n) \end{pmatrix}^{p^s} = \begin{pmatrix} (a_1)^{p^s} & & * \\ & \ddots & \\ * & & (a_n)^{p^s} \end{pmatrix} \quad , \text{ comme on le voit aisément}$$

compte tenu du fait que $p^2 = 0$. Il en résulte que $(a_i)^{p^s} = 1$ pour tout $i=1, \dots, n$ ce qui permet de définir n AG-modules $M_i = A[X]/(Q_i)$, où $Q_i = X^{k_i} - \sum_{j=0}^{k_i-1} a_{ij} X^j$, pour lesquels la matrice de g dans la base $\{1, X, \dots, X^{k_i-1}\}$ est précisément a_i . Par construction des a_i , on a $M_i/pM_i \cong K[X]/(X-1)^{k_i}$ et par le premier cas, $k_i \leq p^{s-1}$ ou $k_i \geq p^s - p^{s-1}$. $\square$

Corollaire 4.10 : Si $G = C_p$ ($s=1$) et si M est un AG-module A-libre de type fini, alors il existe des entiers l, n et n tels que $M/pM \cong (K[X]/(X-1))^l \oplus (K[X]/(X-1)^{p-1})^n \oplus (K[X]/(X-1)^p)^1$.

Preuve : Par la proposition les seules valeurs de k_i pouvant intervenir dans une décomposition en types de M/pM sont ≤ 1 ou $\geq p-1$. En regroupant les facteurs de même type, on obtient le résultat. $\square$

Il serait souhaitable de pouvoir généraliser ce corollaire à s quelconque :
Du 1er cas de la proposition 4.9, il résulte que si $M/pM \cong K[X]/(X-1)^k$, alors $M \cong A[X]/(Q)$, Q divisant $X^{p^s}-1$, et donc k est le degré d'un diviseur de $X^{p^s}-1$.
En particulier, k est le degré d'un diviseur usuel si $r \geq s+1$, par la proposition 4.8. Si M est quelconque et si M/pM contient un facteur de type k , il faudrait pouvoir construire un module N tel que $N/pN \cong K[X]/(X-1)^k$, ce que nous ne savons faire que si $r = 2$ (2ème cas de la proposition). On peut donc énoncer :

Conjecture 1 : Si M est un AG-module A -libre et si $M/pM \cong \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$, alors chaque k_i est le degré d'un polynôme unitaire divisant $X^{p^s}-1$.

Comme les degrés possibles des diviseurs de $X^{p^s}-1$ sont déterminés par la proposition 4.8 et la remarque qui la suit, cette conjecture permettrait de connaître exactement les valeurs de k pouvant intervenir dans une décomposition de M/pM . Lorsque $s = 1$, cette conjecture est vraie en vertu du corollaire 4.10.

La proposition 4.9 montre que si M est un AG-module A -libre, alors $M/pM \cong \left[\bigoplus_{i=1}^n K[X]/(X-1)^{k_i} \right] \oplus \left[\bigoplus_{j=1}^m K[X]/(X-1)^{k_j} \right]$ où $k_i \leq p^{s-1}$ ($i=1, \dots, n$) et $k_j \geq p^{s-p^{s-1}}$ ($j=1, \dots, m$).

Conjecture 2 : Si M est un AG-module A -libre, alors $M = M_1 \oplus M_2$ où $M_1/pM_1 \cong \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$, $k_i \leq p^{s-1}$ ($i=1, \dots, n$) et où $M_2/pM_2 \cong \bigoplus_{j=1}^m K[X]/(X-1)^{k_j}$, $k_j \geq p^{s-p^{s-1}}$ ($j=1, \dots, m$).

On verra plus loin que cette conjecture est vraie dans le cas $s = 1$ (théorème 4.22).

Proposition 4.11 : Si la 2ème conjecture est vraie et si p est impair, alors la première conjecture est vraie. Si $p = 2$, la première conjecture est vraie.

Preuve : Comme M est décomposable en $M = M_1 \oplus M_2$, il suffit de considérer M_1 et M_2 séparément.

1er cas : M est tel que $M/pM \cong \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$ avec $k_i \leq p^{s-1}$ ($i=1, \dots, n$). Comme p est impair, on peut appliquer la proposition 4.5 : $M/p^{r-1}M$ est annihilé par $g^{p^{s-1}-1}$. C'est donc un AH-module $A/p^{r-1}A$ -libre, où $H = C_{p^{s-1}}$. Par récurrence sur s , chaque k_i est le degré d'un polynôme unitaire Q_i divisant $X^{p^{s-1}}-1$ sur $A/p^{r-1}A$. On relève Q_i arbitrairement en un polynôme unitaire de $A[X]$, noté encore Q_i . Par la proposition 4.7, Q_i divise $X^{p^s}-1$. A noter que la récurrence démarre bien car la conjecture 1 est vraie pour $s=1$. Le 2ème cas va se ramener au premier grâce au lemme suivant :

Lemme 4.12 : Soient M un AG-module A -libre et N son complément.

$M/pM \cong \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$ si et seulement si $N/pN \cong \bigoplus_{i=1}^n K[X]/(X-1)^{p^s - k_i}$

Preuve : On a une suite exacte $0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$ où L est la couverture projective de M . L est en fait libre car AG est local (p et $g-1$ engendrent un idéal maximal nilpotent, donc unique). Par la proposition 2.20, L/pL est la couverture projective de M/pM . Or $KG \cong K[X]/(X-1)^{p^s}$ est la couverture projective de $K[X]/(X-1)^{k_i}$ pour tout i , car $\epsilon_i : K[X]/(X-1)^{p^s} \longrightarrow K[X]/(X-1)^{k_i}$ est clairement un revêtement essentiel. Donc $L/pL \cong (KG)^n$.

Comme M est A -libre, la suite $0 \longrightarrow N/pN \longrightarrow L/pL \longrightarrow M/pM \longrightarrow 0$ est exacte, et donc $N/pN \cong \bigoplus_{i=1}^n \text{Ker } \epsilon_i$. Mais KG est un anneau court de longueur p^s et d'uniformisante $X-1$ et il résulte du corollaire de la proposition 1.1 que $\text{Ker } \epsilon_i = (X-1)^{k_i} \cdot (K[X]/(X-1)^{p^s}) \cong K[X]/(X-1)^{p^s - k_i}$.

La réciproque se démontre de manière duale. $\square$

2ème cas : M est tel que $M/pM \cong \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$ avec $k_i \geq p^s - p^{s-1}$ ($i=1, \dots, n$). Par le lemme, le complément N de M satisfait les hypothèses du 1er cas car $p^s - k_i \leq p^{s-1}$. Ainsi $p^s - k_i$ est le degré d'un polynôme unitaire Q_i divisant $X^{p^s} - 1$. Mais alors le polynôme $(X^{p^s} - 1)/Q_i$ divise $X^{p^s} - 1$ et il est de degré k_i , ce qui achève la démonstration dans le cas impair. Le cas $p = 2$ est tout à fait trivial car tout entier positif $k \leq p^s$ est le degré d'un diviseur (même usuel) de $X^{2^s} - 1$ en vertu de la remarque suivant la proposition 4.8. $\square$

Si M/pM contient un facteur de type p^s , c'est-à-dire libre car $K[X]/(X-1)^{p^s} \cong KG$, alors ce facteur peut être relevé en un sous-module N de M , facteur direct dans M . N est d'ailleurs automatiquement libre. Cela résulte en fait d'un résultat tout à fait général sur le relèvement de modules projectifs :

Proposition 4.13 : Soient A un anneau court d'uniformisante π et de corps résiduel K , G un groupe fini, M un AG-module A -libre et Q un sous-module KG -projectif de $M/\pi M$. Alors $M = P \oplus M'$ où P est AG-projectif et $P/\pi P = Q$.

Preuve : Soit P la couverture projective de Q comme AG-module. $P/\pi P \cong Q$ en vertu de la proposition 3.1. Comme Q est KG -projectif, il est KG -injectif

et donc $M/\pi M = N \oplus Q$. Vu que P est projectif, il existe $f : P \rightarrow M$ faisant commuter le diagramme

$$\begin{array}{ccc} M & \xleftarrow{f} & P \\ \downarrow & & \downarrow \\ M/\pi M & \xrightarrow{p} & Q \end{array}$$

Alors la réduction mod π $\bar{f}$ de f est une section de p , donc injective. Via les isomorphismes $M/\pi M \cong \pi^{r-1}M$ et $P/\pi P \cong \pi^{r-1}P$, $\bar{f}$ n'est autre que $f|_{\pi^{r-1}P}$. $f|_{\pi^{r-1}P}$ est donc injective, ce qui implique immédiatement que f l'est. Ainsi P s'identifie à un sous-module de M , facteur direct dans M car P est AG-injectif. $\square$

§3 Classification des modules de type k .

Nous allons maintenant étudier de plus près la structure des modules de type k où k est le degré d'un diviseur unitaire de $X^{p^s}-1$. Dans l'optique de la classification de tous les AG-modules, cela ne donnera bien sûr que des résultats partiels car d'une part la restriction sur k dépend de la conjecture 1 et d'autre part un AG-module A -libre quelconque ne se décompose pas nécessairement en somme directe de modules de type k . Nous verrons d'ailleurs même un contre-exemple dans le cas $s \geq 2$ au paragraphe suivant.

Nous dirons simplement qu'un module M est de type k si M est un A -module A -libre de type k . k sera toujours le degré d'un diviseur unitaire Q de $X^{p^s}-1$, conformément à la conjecture 1. En considérant au besoin le complément du module, on peut supposer $k \leq p^{s-1}$ en vertu de la proposition 4.4 et du lemme 4.12. Plus précisément :

Proposition 4.14 : Soient M un module de type k et N son complément. On suppose $k \neq p^s$.

(1) N est de type p^{s-k} .

(2) M est indécomposable si et seulement si N l'est.

(3) Le passage au complément induit une bijection de l'ensemble des classes d'isomorphisme de modules de type k sur l'ensemble des classes d'isomorphisme de modules de type p^{s-k} .

(4) Soit Q un diviseur unitaire de degré k de $X^{p^s}-1$ et $R = (X^{p^s}-1)/Q$. Alors, pour $0 \leq e \leq r$: $QM \subset p^e M$ si et seulement si $RN \subset p^e N$.

Preuve : {1} résulte du lemme 4.12.

{2} Résulte de la proposition 2.22 car, comme $k \neq p^s$, M est sans facteur projectif.

{3} Par la proposition 2.22, le passage au complément induit une bijection de l'ensemble des classes d'isomorphisme de AG-modules sans facteur projectif sur lui-même. Reste à voir que l'image des modules de type k est exactement formée des modules de type $p^s - k$. Or si N est de type $p^s - k$, N est le complément d'un certain module M , qui doit être de type k en vertu du lemme 4.12.

{4} $QM \subset p^e M \Leftrightarrow Q(M/p^e M) = 0$, donc quitte à travailler sur $A/p^e A$, on peut supposer $e = r$. Il s'agit donc de montrer : $QM = 0 \Leftrightarrow RN = 0$.

Lemme 4.15 : $QM = 0 \Leftrightarrow M$ est un B -module libre, où $B = A[X]/(Q)$.

En effet, si $QM = 0$, M est clairement un B -module. Comme $Q = (X-1)^k \bmod p$, $B/pB \cong K[X]/(X-1)^k$ et comme M est de type k , M/pM est un B/pB -module libre, d'un certain rang n . Il en résulte alors que M est B -libre car si P est la couverture projective de M comme B -module, alors P est aussi la couverture projective de M/pM , car $M \rightarrow M/pM$ est un revêtement essentiel, et donc P est B -libre de rang n . Mais alors la surjection $P \rightarrow M$ est un isomorphisme car P et M sont A -libres de même rang nk .

Il résulte de ces préliminaires qu'il suffit de montrer que M est un B -module libre si et seulement si N est un C -module libre où $C = A[X]/(R)$.

Or ceci découle immédiatement du fait que le complément de B , considéré comme AG-module, est isomorphe à C , considéré aussi comme AG-module : On a une suite exacte $0 \rightarrow Q \cdot A[X]/(X^{p^s} - 1) \rightarrow A[X]/(X^{p^s} - 1) \rightarrow A[X]/(Q) \rightarrow 0$. Comme $Q \cdot R = X^{p^s} - 1$, la multiplication par $Q : A[X] \rightarrow Q \cdot A[X]$ induit un isomorphisme $A[X]/(R) \xrightarrow{\sim} Q \cdot A[X]/(Q \cdot R) = Q \cdot A[X]/(X^{p^s} - 1)$. $\square$

Si M est un module de type k et si Q est un diviseur unitaire de degré k de $X^{p^s} - 1$, alors $QM \subset pM$ car $Q \equiv (X-1)^k \bmod p$ et $(X-1)^k M/pM = 0$ par définition du type k . On a vu dans la proposition 4.5 que si $Q = X^{p^s-1} - 1$, alors on a même $QM \subset p^{r-1}M$. La proposition suivante généralise ce résultat en déterminant la plus grande puissance e de p telle que $QM \subset p^e M$.

Proposition 4.16 : Soient M un module de type k et Q un diviseur unitaire de degré k de $X^{p^s}-1$. On suppose p impair. Alors $QM \subset p^e M$ où $e = \max(1, r-s+v_p(k))$, $v_p(k)$ désignant la valuation p -adique de k . En particulier $e = r-s+v_p(k)$ si $r \geq s+1$.

Preuve : Comme $1 \leq k \leq p^s$, $0 \leq v_p(k) \leq s$ et par conséquent $s \geq s-v_p(k) \geq 0$, ce qui démontre le cas particulier car, si $r \geq s+1$, $r-s+v_p(k) \geq v_p(k)+1 \geq 1$. On procède par récurrence sur s . Si $s = 0$, alors le groupe est trivial, $Q = X-1$ et $k = 1$. Comme X agit par l'identité, $QM = 0 = p^r M$ et on a bien $r = r-s+v_p(k)$. Si maintenant $s \geq 1$, on exclut d'abord le cas $k = p^s$ qui est évident : le seul diviseur unitaire de degré p^s de $X^{p^s}-1$ est $Q = X^{p^s}-1$. $QM = 0 = p^r M$ et on a bien $r = r-s+v_p(k)$ car $v_p(k) = s$.

En vertu de la proposition 4.3, $k \leq p^{s-1}$ ou $k \geq p^s-p^{s-1}$. Dans le second cas, on considère le complément $\bar{k}$ de M , qui est de type $p^s-k \leq p^{s-1}$, et il suffit de montrer que $R\bar{N} \subset p^e \bar{N}$, où $R = (X^{p^s}-1)/Q$, en vertu de la proposition 4.14 et du fait que $v_p(p^s-k) = v_p(k)$ ($0 < k < p^s$). On peut donc supposer $k \leq p^{s-1}$.

Par la proposition 4.5 et le fait que p est impair, $(X^{p^{s-1}}-1)M \subset p^{r-1}M$. Donc $M_1 = M/p^{r-1}M$ est un $(A/p^{r-1}A)$ -module de type k où $H = C_p^{s-1}$. De plus Q divise $X^{p^{s-1}}-1$ sur l'anneau $A/p^{r-1}A$ en vertu de la proposition 4.7. Par hypothèse de récurrence $QM_1 \subset p^e M_1$ car $(r-1) - (s-1) + v_p(k) = r-s + v_p(k)$. Il en résulte immédiatement que $QM \subset p^e M$. A noter que comme on a toujours supposé $r \geq 2$, la récurrence ne s'applique que si $r-1 \geq 2$ et il faut donc traiter à part le cas $r = 2$. Mais ce cas est trivial car, comme $k < p^s$, $v_p(k) < s$, $r-s+v_p(k) < r=2$, $e = \max(1, r-s+v_p(k)) = 1$, et $QM \subset pM$ par définition du type k . $\square$

k étant fixé, on choisit une fois pour toutes un diviseur unitaire Q de degré k de $X^{p^s}-1$. Si $r \geq s+1$, on choisira par exemple Q un diviseur usuel de $X^{p^s}-1$ (proposition 4.8). L'exemple type de module de type k est alors $(A[X]/(Q))^n$, qui est annulé par Q . Pour décrire un module de type k quelconque M , on examine alors de combien la multiplication par Q dans M s'éloigne de zéro.

On pose $e = \max(1, r-s + v_p(k))$ et on définit $\phi: p^e M \rightarrow p^e M$ par $\phi(p^e x) = Qx$. ϕ est bien défini car si $p^e x = p^e y$, alors $x-y \in M(p^e) = p^{r-e} M$.

Comme Q annule $M/p^e M \cong p^{r-e} M$, $Q(x-y) = 0$, donc $\phi(p^e x) = \phi(p^e y)$. De plus l'image de ϕ est bien contenue dans $p^e M$ car $QM \subset p^e M$. ϕ est un endomorphisme AG-linéaire de $p^e M$ car g commute à Q vu que Q est un polynôme en g . Nous appellerons ϕ l'endomorphisme caractéristique du module M .

Si Q agit par zéro dans $p^e M$, alors, comme $p^e M \cong M/p^{r-e} M$, $p^e M$ est un B -module libre, où $B = (A/p^{r-e} A)[X]/(Q)$, en vertu du lemme 4.15. Nous ferons l'hypothèse $Qp^e M = 0$, car ainsi la structure de AG-module de $p^e M$ est connue, ce qui va permettre de classer les modules de type k à l'aide de leur endomorphisme caractéristique. Comme $M/p^e M \cong p^{r-e} M$, $Qp^{r-e} M = 0$ et pour que $Qp^e M = 0$, il suffit que $p^e M \subset p^{r-e} M$, i.e. $e \geq r-e$. Cette condition donne $r = 2$ si $e = 1$, et $r \geq 2$ ($s-v_p(k)$) si $e = r-s+v_p(k)$. Si l'on veut une condition uniforme pour tous les types à la fois, on peut supposer $r = 2$ ou $r \geq 2s$.

Ainsi $p^e M$ est un B -module libre muni d'un endomorphisme ϕ , c'est-à-dire un $B[Y]$ -module, Y agissant par ϕ . Si $f : M \rightarrow N$ est un homomorphisme de modules de type k , alors $\bar{f} = f|_{p^e M} : p^e M \rightarrow p^e N$ est $B[Y]$ -linéaire car : $\bar{f}(\phi(p^e x)) = f(Qx) = Qf(x) = \phi p^e f(x) = \phi \bar{f}(p^e x)$, ϕ étant l'endomorphisme caractéristique de N . On obtient ainsi un foncteur de la catégorie des modules de type k dans la catégorie des $B[Y]$ -modules, B -libres de type fini. Ce foncteur est exact dans le sens que, si $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ est une suite exacte de modules de type k , alors la suite de $B[Y]$ -modules $0 \rightarrow p^e M' \rightarrow p^e M \rightarrow p^e M'' \rightarrow 0$ est aussi exacte, ce qui découle immédiatement du fait que M'' est A -libre.

Lemme : Soient M et N deux modules de type k et $\bar{f} : p^e M \rightarrow p^e N$ un homomorphisme $B[Y]$ -linéaire. Alors :

- (1) Il existe un homomorphisme AG-linéaire $f : M \rightarrow N$ tel que $f|_{p^e M} = \bar{f}$.
- (2) f est injectif (respectivement surjectif) $\iff \bar{f}$ est injectif (respectivement surjectif).

Preuve : (1) Si $\{p^e x_1, \dots, p^e x_n\}$ est une base de $p^e M$ comme B -module, alors $\{p^e g^i x_j \mid 0 \leq i \leq k-1, 1 \leq j \leq n\}$ est une $A/p^{r-e} A$ -base de $p^e M$. Alors $\{g^i x_j \mid 0 \leq i \leq k-1, 1 \leq j \leq n\}$ est une A -base de M .

Si $\bar{f}(p^e x_j) = p^e y_j$, on définit $f(g^i x_j) = g^i y_j$, $0 \leq i \leq k-1$. Pour que f soit AG-linéaire, il reste à vérifier que $gf(g^{k-1} x_j) = f(g^k x_j)$. Or si $Q = x^k - \sum_{i=0}^{k-1} a_i x^i$, $f(g^k x_j) = \sum_{i=0}^{k-1} f(a_i g^i x_j) + f(Qx_j) = \sum_{i=0}^{k-1} a_i g^i f(x_j) + f(Qx_j)$.

Or $f(Qx_j) = f(Yp^e x_j) = \tilde{f}(Yp^e x_j) = Y \tilde{f}(p^e x_j) = Y p^e f(x_j) = Qf(x_j)$ par définition de l'endomorphisme caractéristique (multiplication par Y) et par le fait que $\tilde{f}$ commute à Y par hypothèse. On en déduit donc :

$$f(g^k x_j) = \sum_{i=0}^{k-1} a_i g^i f(x_j) + Qf(x_j) = g^k f(x_j) = gf(g^{k-1} x_j).$$

(2) L'implication $\Rightarrow$ est évidente par exactitude du foncteur défini ci-dessus. Vu que, via l'isomorphisme $p^e M \cong M/p^{r-e} M$, $\tilde{f}$ n'est autre que la réduction modulo p^{r-e} de f , alors f est surjective si $\tilde{f}$ l'est par le lemme de Nakayama. Si $\tilde{f}$ est injective et si $x \in \text{Ker } f$ est non nul, il existe $t < r$ tel que $p^t x \neq 0$ et $p^{t+1} x = 0$. Alors $p^t x \in M(p) = p^{r-1} M \subset p^e M$ et donc $p^t x \in \text{Ker } f \cap p^e M = \text{Ker } \tilde{f} = 0$, contrairement au choix de t . $\square$

Théorème 4.17 : Soient Q un diviseur unitaire de degré k de $X^{p^s} - 1$, $R = (X^{p^s} - 1)/Q$, $e = \max \{1, r-s + v_p(k)\}$, $B = (A/p^{r-e} A)[X]/(Q)$, M et M' deux AG-modules de type k . On suppose p impair, on suppose aussi $r = 2$ ou $r \geq 2$ ($s - v_p(k)$). Alors :

(1) $p^e M$ est un $B[Y]$ -module B -libre, où la multiplication par Y est l'endomorphisme caractéristique de M .

(2) $M \cong M'$ si et seulement si $p^e M \cong p^e M'$ comme $B[Y]$ -modules.

(3) M est irréductible comme module de type k si et seulement si $p^e M$ est irréductible comme $B[Y]$ -module B -libre.

(4) M est indécomposable si et seulement si $p^e M$ est indécomposable comme $B[Y]$ -module.

(5) Soit $\bar{N}$ un $B[Y]$ -module, B -libre de type fini. Il existe un module N de type k tel que $p^e N \cong \bar{N}$ comme $B[Y]$ -modules si et seulement si $R \cdot \text{Im } Y = 0$ dans $\bar{N}$.

Preuve : (1) n'est qu'un rappel de ce qu'on a déjà vu et (2) est immédiat par le lemme. Montrons (5). Si N existe, alors par définition même de l'endomorphisme caractéristique de N , $QN = \text{Im } Y \subset p^e N$. Alors $R \cdot \text{Im } Y = RQN = (X^{p^s} - 1)N = 0$. Réciproquement, Si $\bar{N}$ est B -libre de base $x_1, \dots, x_n$, soit N un $A[X]/(Q)$ -module libre de base $y_1, \dots, y_n$. Alors $p^e N \cong N/p^{r-e} N \cong \bar{N}$ comme B -modules. N est bien sûr un AG-module mais on va définir sur N une nouvelle structure de AG-module qui coïncidera avec la première sur $p^e N$, n'altérant donc pas l'isomorphisme $p^e N \cong \bar{N}$. On dénotera par $\phi : p^e N \rightarrow p^e N$ l'endomorphisme de multiplication par Y , transporté de $\bar{N}$ dans $p^e N$.

N admet comme A-base $\{X^i y_j \mid 0 \leq i \leq k-1, 1 \leq j \leq n\}$ et si $Q = X^k - \sum_{i=0}^{k-1} a_i X^i$, alors $X \cdot X^{k-1} y_j = \sum_{i=0}^{k-1} a_i X^i y_j$. On définit alors une action de G par : $g X^i y_j = X^{i+1} y_j$ si $i < k-1$ et $g X^{k-1} y_j = \sum_{i=0}^{k-1} a_i X^i y_j + \phi(p^e y_j)$. g coïncide donc avec X sur les k-1 premiers vecteurs de base (pour chaque j). Pour vérifier que les actions de X et de g coïncident sur $p^e N$, il s'agit de montrer que $p^e \phi(p^e y_j) = 0$. Or $\phi(p^e y_j) \in p^e N$ et il suffit de montrer que $p^{2e} N = 0$, c'est-à-dire $2e \geq r$. C'est clair si $r = 2$, car alors $e = 1$. Sinon, la condition $2e \geq r$ est équivalente à notre hypothèse $r \geq 2(s-v_p(k))$ car $e = r-s+v_p(k)$. Maintenant $\phi(p^e y_j) = g X^{k-1} y_j - \sum_{i=0}^{k-1} a_i X^i y_j = (g^k - \sum_{i=0}^{k-1} a_i g^i) y_j = Q(g) y_j$. Donc $(g^{p^s}-1) y_j = R(g) Q(g) y_j = R(g) \phi(p^e y_j) = R(X) \phi(p^e y_j) = 0$ car $R(g) = R(X)$ sur $p^e N$ et $R(X) \text{Im} \phi = 0$ par hypothèse. Il s'agit donc bien d'une action du groupe G. De plus l'égalité $\phi(p^e y_j) = Q(g) y_j$ montre que ϕ est l'endomorphisme caractéristique de N et par conséquent que la structure de $B[Y]$ -module de $p^e N$ donnée par l'endomorphisme caractéristique coïncide bien avec la structure de $B[Y]$ -module donnée sur $\bar{N}$.

(3) et (4) vont résulter de l'assertion suivante :

Si $\bar{N}$ est un sous- $B[Y]$ -module B-libre de $p^e M$, alors il existe un sous-module N de type k de M tel que $p^e N = \bar{N}$. En effet, par (5), $R \cdot \text{Im} Y = 0$ dans $p^e M$ et donc $R \cdot \text{Im} Y = 0$ dans $\bar{N}$. Par (5) encore, il existe un module N de type k tel que $p^e N \cong \bar{N}$. Par le lemme, il existe une injection $f : N \rightarrow M$ relevant l'injection $\bar{f} : p^e N \cong \bar{N} \hookrightarrow p^e M$. $f(N)$ est alors un sous-module de type k de M tel que $p^e f(N) = \bar{N}$.

(3) Précisons qu'un module de type k est irréductible comme module de type k s'il n'admet pas de sous-module propre de type k (en particulier A-libre). Cela ne signifie pas qu'il soit irréductible comme AG-module car il pourrait posséder un sous-AG-module A-libre de type différent de k. De même un $B[Y]$ -module B-libre est irréductible s'il n'admet pas de sous- $B[Y]$ -module B-libre propre non nul. Si N est un sous-module de type k de M, alors $p^e N$ est clairement un sous- $B[Y]$ -module B-libre de $p^e M$. Donc $p^e M$ est irréductible si M l'est. La réciproque découle immédiatement de l'assertion.

(4) Si M est décomposable, $M = M_1 \oplus M_2$, alors $p^e M = p^e M_1 \oplus p^e M_2$ est clairement une décomposition de $p^e M$ comme $B[Y]$ -module. En fait M_1 et M_2 sont forcément de type k et $p^e M_1$ et $p^e M_2$ sont B-libres.

Réciproquement, si $p^e M = \bar{N}_1 \oplus \bar{N}_2$, $\bar{N}_1$ et $\bar{N}_2$ sont B-projectifs, donc B-libres car B est local (p est nilpotent et B/pB est local d'idéal maximal (X-1)). Il résulte alors de l'assertion qu'il existe des sous-modules de type k N_1 et N_2 de M tels que $p^e N_i = \bar{N}_i$ (i=1,2). $N_1 \cap N_2 = 0$ car $\bar{N}_1 \cap \bar{N}_2 = 0$. Si f est l'injection de $N_1 \oplus N_2$ dans M, $\tilde{f} : \bar{N}_1 \oplus \bar{N}_2 \rightarrow p^e M$ est surjective, donc f aussi en vertu du lemme. $\square$

(5) montre qu'on a en fait un foncteur F de la catégorie $\underline{K}$ des modules de type k dans la catégorie $\underline{Y}$ des $B[Y]$ -modules, B-libres de type fini annihilés par RY, R désignant bien sûr l'image dans B du polynôme $R \in A[X]$. On n'a pas une équivalence de catégories car il y a "trop" de morphismes dans $\underline{K}$ pour qu'on puisse définir sans équivoque l'image d'un morphisme par un foncteur (hypothétique!) de $\underline{Y}$ dans $\underline{K}$. Il n'y a en revanche pas de problème pour les objets en vertu de (5). On peut néanmoins trouver une équivalence de catégories entre $\underline{K}'$ et $\underline{Y}$ où $\underline{K}'$ est la catégorie ayant les mêmes objets que $\underline{K}$ et ayant pour morphismes les classes d'équivalence de morphismes de $\underline{K}$ pour la relation :

$$f, g : M \rightarrow M', \quad f \sim g \iff f|_{p^e M} = g|_{p^e M}.$$

De toute façon, le foncteur $\tilde{F}$ induit une application F de l'ensemble des classes d'isomorphisme de modules de type k dans l'ensemble des classes d'isomorphisme de $B[Y]$ -modules, B-libres de type fini, annihilés par RY (qu'on peut voir encore comme des $B[Y]/(RY)$ -modules). Le théorème affirme que $\tilde{F}$ est une bijection préservant les indécomposables et les irréductibles. La classification des modules de type k se réduit donc à celle des $B[Y]$ -modules B-libres de type fini annihilés par RY. Si la classification de ces modules à isomorphisme près n'est pas toujours aisée, selon la nature de B, on sait néanmoins qu'ils sont donnés par une matrice dans $M_n(B)$, annihilée par R, ce qui permet de construire aisément des modules de type k.

Exemples : 1) $k = p^{s-1}$, $v_p(k) = s-1$, $e = r-s+v_p(k) = r-1$. A remarquer que la condition $r \geq 2(s-v_p(k))$ se réduit dans ce cas à $r \geq 2$, ce qu'on a toujours supposé. $Q = Xp^{s-1} - 1$ et $B = K[X]/(Q) = K[X]/(X-1)p^{s-1}$. B est dans ce cas l'algèbre du groupe cyclique $C_{p^{s-1}}$ sur K. La condition $RY = 0$ est automatiquement satisfaite car R annule B.

$R = \sum_{k=0}^{p-1} X^k p^{s-1} \equiv (X-1)^{(p-1)p^{s-1}} \pmod{p}$. Comme $(p-1)p^{s-1} > p^{s-1}$, $RB = 0$. Ainsi la classification des modules de type p^{s-1} est équivalente à celle des $K[X, Y]/(X-1)p^{s-1}$ -modules, $K[X]/(X-1)p^{s-1}$ -libres de type fini.

En particulier, si $s = 1$, alors $k = p^{s-1} = 1$ et $B = K[X]/(X-1) \cong K$. Donc les AC_p -modules de type 1 se classent comme les $K[Y]$ -modules de dimension finie sur K . Nous y reviendrons au §6.

2) $k = 1$, $v_p(k) = 0$, $e = r-s$. On suppose $r \geq 2s$. $Q = X-1$ et $B = (A/p^s A)[X]/(X-1) \cong A/p^s A$. La condition $RY = 0$ est à nouveau automatiquement satisfaite car R annule B . $R = \sum_{k=0}^{p^s-1} C^k$ et comme X agit par l'identité dans B , $RB = p^e B = 0$. La classification des modules de type 1 est équivalente à celle des $(A/p^s A)[Y]$ -modules $A/p^s A$ -libres de type fini.

Lorsque $s = 1$, on retrouve le cas particulier de l'exemple 1.

A remarquer que la situation est particulièrement simple dans ces deux exemples car B est chaque fois un anneau court, ce qui est loin d'être le cas en général.

3) En vertu du 1er cas de la preuve de la proposition 4.9, on sait que si M est un module de type k tel que $M/pM = K[X]/(X-1)^k$, alors $M \cong A[X]/(Q_1)$ où Q_1 est un diviseur unitaire de degré k de X^{p^s-1} . La condition sur M/pM est équivalente à la suivante : $p^e M$ est B -libre de rang 1. Donc, pour trouver tous les diviseurs unitaires Q_1 de degré k de X^{p^s-1} , connaissant l'un d'entre eux Q , il s'agit de déterminer les endomorphismes B -linéaires Y de $B = (A/p^{r-e} A)[X]/(Q)$ tels que $RY = 0$. Un tel endomorphisme est bien sûr déterminé par l'image P de $1 \in B$, et P doit être dans le noyau de R . P admet un représentant unique de degré $\leq k-1$ dans $(A/p^{r-e} A)[X]$, et par l'isomorphisme $M/p^{r-e} M \cong p^e M$, P est envoyé sur $p^e P_0$ où P_0 est un polynôme dans $A[X]$ dont la réduction modulo p^{r-e} est P . Si x désigne la classe de 1 dans $M = A[X]/(Q_1)$, alors $Qx = \phi(p^e x)$, ϕ étant l'endomorphisme caractéristique de M . Par l'isomorphisme $B \cong p^e M$, 1 est envoyé sur $p^e x$ et par conséquent P sur $p^e P_0 x$. Donc $\phi(p^e x) = p^e P_0 x$ et $(Q-p^e P_0)x = 0$, ce qui implique $Q_1 = Q-p^e P_0$ car les 2 polynômes sont unitaires de degré k .

En résumé, si Q est un diviseur unitaire de degré k de X^{p^s-1} , et si $r \geq 2(s-v_p(k))$ (ou $r=2$), alors tout diviseur unitaire de degré k de X^{p^s-1} est de la forme $Q-p^e P_0$ où P_0 est un polynôme de degré $\leq k-1$ dont la classe P dans $(A/p^{r-e} A)[X]/(Q)$ est

annulées par $R = (X^{p^s} - 1)/Q$. Réciproquement, si $PR = 0$, cela signifie que $RP_0 \in (p^{r-e}, Q)$, donc que $p^e R \cdot P_0 = p^e Q S_0$ pour un certain S_0 . On sait qu'à partir de P , on peut reconstruire un endomorphisme de B , donc un module de la forme $A[X]/(Q_1)$, c'est-à-dire un diviseur unitaire $Q_1 = Q - p^e P_0$. On vérifie aussi directement que Q_1 divise $X^{p^s-1} : (Q - p^e P_0)(R + p^e S_0) = QR - p^e RP_0 + p^e QS_0 = X^{p^s-1}$, compte tenu du fait que $p^{2e} = 0$ vu que $2e \geq r$.

Si par exemple $k = p^{s-1}$, on a vu dans l'exemple 1 que la condition $RY = 0$ est toujours satisfaite et que $e = r-1$. $Q = X^{p^s-1}$ et les diviseurs unitaires de degré p^{s-1} sont les polynômes $Q - p^{r-1} P_0$ où P_0 est un polynôme quelconque de degré $\leq p^{s-1}-1$. Lorsque $s = 1$, ceci démontre les affirmations de la remarque suivant la proposition 4.4.

§ 4 Endomorphisme caractéristique global.

Au paragraphe précédent, on n'a considéré que des modules de type k mais il est néanmoins possible de définir un endomorphisme caractéristique "global" pour certains modules de type "composé" : Si M est un AG-module A-libre tel que $M/pM \cong \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$, chaque k_i étant inférieur ou égal à p^{s-1} , on dira que M est un module de type composé $\leq p^{s-1}$.

La conjecture 2 affirme que tout AG-module A-libre M se décompose en $M = M_1 \oplus M_2$ où M_1 est de type composé $\leq p^{s-1}$ et M_2 de type composé $\geq p^s - p^{s-1}$. Comme le complément N de M_2 est de type composé $\leq p^{s-1}$ en vertu du lemme 4.12 et que la connaissance de N détermine entièrement celle de M_2 (proposition 2.22), il n'est pas du tout restrictif de ne considérer que les modules de type composé $\leq p^{s-1}$, pour autant que la conjecture soit vraie.

Si p est impair, et si M est de type composé $\leq p^{s-1}$, il résulte de la proposition 4.5 que $(g^{p^{s-1}} - 1)M \subset p^{r-1}M$. On définit alors l'endomorphisme caractéristique (global) de M : $\phi : p^{r-1}M \rightarrow p^{r-1}M$, $\phi(p^{r-1}x) = (g^{p^{s-1}} - 1)x$. On vérifie aisément que ϕ est bien défini et que c'est un endomorphisme AG-linéaire. Si $B = KC_{p^{s-1}} \cong K[X]/(X-1)^{p^{s-1}}$, $p^{r-1}M \cong M/pM$ est un B -module muni d'un endomorphisme, donc un $B[Y]$ -module, de type fini comme B -module. A remarquer que si M est un module de type $k \leq p^{s-1}$, cet endomorphisme ne coïncide avec l'endomorphisme caractéristique défini au paragraphe précédent que si $k = p^{s-1}$, auquel cas $p^{r-1}M$ est un B -module libre.

Cette construction définit un foncteur de la catégorie des modules de type composé $\leq p^{s-1}$, dans la catégorie des $B[Y]$ -modules, de type fini comme B -modules. Ce foncteur est exact et, si $M \cong M'$, alors $p^{r-1}M \cong p^{r-1}M'$ comme $B[Y]$ -modules. L'endomorphisme caractéristique de M est donc un invariant de la classe d'isomorphisme de M mais l'analogie avec le paragraphe 3 s'arrête là car la classe d'isomorphisme de M n'est cette fois plus déterminée par cet invariant. Si par exemple $M = A$ avec action triviale de G et $M' = A$ avec l'action de G suivante : $gx = x + p^{r-1}x$, alors on vérifie aisément que $g^p x = x$ et par conséquent $(g^{p^{s-1}} - 1)M' = 0$, si s est supposé ≥ 2 . Ainsi l'endomorphisme caractéristique est nul dans les deux cas alors que $M \not\cong M'$.

Proposition 4.18 : On suppose $r \geq 2s$. Soit N un $B[Y]$ -module $N = \bigoplus_{i=1}^n K[X]/(X-1)^{k_i}$, $k_i \leq p^{s-1}$. Dénotons par ϕ l'endomorphisme de multiplication par Y .

On suppose que k_i est le degré d'un diviseur unitaire Q_i de $X^{p^{s-1}} - 1$ (on peut prendre Q_i diviseur usuel car $r \geq s+1$). Soit $R_i = (X^{p^{s-1}} - 1)/Q_i$. Soit encore $\bar{M} = \bigoplus_{i=1}^n (A/p^{r-s}A)[X]/(Q_i)$ et notons y_i la classe de 1 dans la i ème composante de $\bar{M}$. Il existe un AG -module M de type composé $\leq p^{s-1}$ tel que

(1) $M/p^{r-s}M \cong \bar{M}$ et (2) $p^{r-1}M \cong N$ comme $B[Y]$ -module, si et seulement si $\phi(p^{r-s-1}y_i) = R_i z_i$ pour un certain $z_i \in p^{r-2s}\bar{M}$, où ϕ est vu comme endomorphisme de $p^{r-s-1}\bar{M} \cong N$.

Remarque : Si M est de type k , la condition (1) est automatiquement satisfaite en vertu de la proposition 4.16. On peut faire la conjecture que (1) est toujours réalisé pour un module de type composé quelconque, auquel cas cette proposition donnerait exactement la condition pour que M existe lorsque l'endomorphisme ϕ de $p^{r-1}M$ est donné.

Preuve : Si M existe, M admet comme base $\{g^i x_j \mid 1 \leq i \leq n, 0 \leq j \leq k_i - 1\}$ où l'image de x_i dans $M/p^{r-s}M \cong \bar{M}$ est y_i . Comme $Q_i y_i = 0$, $Q_i x_i \in p^{r-s}M$. Par l'isomorphisme $p^s M \cong M/p^{r-s}M \cong \bar{M}$, $p^s x_i$ est appliqué sur y_i , $p^{r-s}M$ sur $p^{r-2s}\bar{M}$ ($r \geq 2s$), et donc $Q_i x_i$ sur un certain $z_i \in p^{r-2s}\bar{M}$.

Or on a $R_i Q_i x_i = (g^{p^{s-1}} - 1)x_i = \psi(p^{r-1}x_i)$ où ψ est l'endomorphisme caractéristique de M . Comme ψ correspond à ϕ par l'isomorphisme $p^{r-1}M = p^{r-s-1}\bar{M}$, on en déduit $\phi(p^{r-s-1}y_i) = R_i z_i$.

Réciproquement, on définit M comme un A -module libre de base $\{g^i x_1 \mid 1 \leq i \leq n, 0 \leq j \leq k_1 - 1\}$ et il reste à définir $g(g^{k_1-1} x_1)$. Or $g^{k_1} x_1 = Q_1 x_1 - \sum_{j=0}^{k_1-1} a_j g^j x_1$, où $Q_1 = X^{k_1} + \sum_{j=0}^{k_1-1} a_j X^j$. Il suffit donc de définir $Q_1 x_1$. On aura $Q_1 x_1 \in p^{r-s} M$. Donc $p^s M \cong M/p^{r-s} M \cong \bar{M}$. Par hypothèse, il existe $z_1 \in p^{r-s} M$ tel que $R_1 z_1 = \phi(p^{r-1} x_1)$, où ϕ est l'endomorphisme de $p^{r-s-1} \bar{M}$ transporté sur $p^{r-1} M$. On pose $Q_1 x_1 = z_1$ et on a alors $(g^{p^{s-1}-1}) x_1 = R_1 Q_1 x_1 = \phi(p^{r-1} x_1)$ (*). Comme $g^{p^{s-1}-1}$ agit trivialement sur $p^{r-1} M$ vu que chaque k_1 est inférieur ou égal à p^{s-1} , on a $(g^{p^{s-1}-1}) x_1 = (\sum_{k=0}^{p-1} g^{kp^{s-1}})(g^{p^{s-1}-1}) x_1 = p \cdot \phi(p^{r-1} x_1) = 0$, ce qui montre que M est bien un AG-module. La formule (*) montre que ϕ est l'endomorphisme caractéristique de M , ce qui montre (2). $\square$

§5 Décomposition en types.

Il résulte du corollaire 4.10 que si $s = 1$, tout AG-module A -libre de type fini M est tel que $M/pM = N_1 \oplus N_{p-1} \oplus N_p$ où N_k est de type k ($k=1, p-1, p$).

Le but de ce paragraphe est de montrer que M lui-même se décompose en somme directe $M = M_1 \oplus M_{p-1} \oplus M_p$ où M_k est de type k ($k=1, p-1, p$).

C'est un résultat spécifique au cas $s = 1$. Nous verrons des contre-exemples pour $s \geq 2$. Dans le cas $A = \mathbb{Z}/p^r \mathbb{Z}$, ce résultat a été montré par V.S. Drobotenko, E.S. Drobotenko, Z.P. Zhilinskaya et E.V. Pogorilyak en termes de représentations matricielles [DDZP], puis généralisé à un p -anneau court non ramifié quelconque par T. Hannula [Ha 1]. Nous en présentons ici une nouvelle démonstration.

Il résulte de la proposition 4.13 que M contient déjà un facteur direct de type p :

$M = M' \oplus M_p$ avec $M_p/pM_p = N_p$ et $M'/pM' \cong N_1 \oplus N_{p-1}$. On supposera donc $M/pM = N_1 \oplus N_{p-1}$ et on va montrer qu'il existe une autre décomposition en types $M/pM = N'_1 \oplus N'_{p-1}$ qui se relève en une décomposition de M . Par ailleurs, il s'avère beaucoup plus agréable de travailler avec des sous-modules plutôt qu'avec des quotients, et nous allons donc chercher, en vertu de l'isomorphisme $M/pM \cong p^{r-1} M$, à relever une décomposition de $p^{r-1} M$. On suppose encore p impair, le cas $p = 2$ devant être traité à part (§7).

Lemme 4.19 : $\sum_{k=0}^{p-1} X^k = \sum_{k=0}^{p-1} \binom{p}{k+1} (X-1)^k$.

Preuve : $(X-1) \left(\sum_{k=0}^{p-1} X^k \right) = X^{p-1} = ((X-1)+1)^{p-1} = \sum_{k=1}^p \binom{p}{k} (X-1)^k =$
 $= (X-1) \sum_{k=0}^{p-1} \binom{p}{k+1} (X-1)^k$ et le résultat en découle par division par $X-1$. $\square$

Lemme 4.20 : Soit M un AC_p -module A -libre tel que $p^{r-1}M = N_1 \oplus N_{p-1}$ où N_k est de type k . Soit L un sous-module de pM qu'on suppose $A/p^{r-1}A$ -libre et de type $p-1$. Si $x \in \text{Ker}(g-1)^{p-1}$ et si $px \in L$, alors $px = 0$.

Preuve : 1er cas : $r = 2$. Par le lemme 4.19, $0 = (g-1)^{p-1}x = \left(\sum_{k=0}^{p-1} g^k \right)x - \sum_{k=0}^{p-2} \binom{p}{k+1} (g-1)^k x$. On a $(g-1)px = 0$. En effet, si s est le plus grand entier tel que $(g-1)^s px \neq 0$ et si $s \geq 1$, alors, comme $(g-1) \left(\sum_{k=0}^{p-1} g^k \right) = g^{p-1} = 0$ et comme p divise $\binom{p}{k+1}$, on a :
 $0 = (g-1)^s (g-1)^{p-1} x = - \sum_{k=0}^{p-2} \binom{p}{k+1} (g-1)^{k+s} x = -p(g-1)^s x$.
 Ceci contredit la définition de s .

Maintenant, comme $r = 2$, L est un KC_p -module de type $p-1$, c'est-à-dire un $K[X]/(X-1)^{p-1}$ -module libre. Par la proposition 1.1, $L(g-1) = (g-1)^{p-2}L$. Donc, comme $px \in L$ et que $(g-1)px = 0$, $px = (g-1)^{p-2}y$ pour un $y \in L$. Comme $L \subset pM$, $y = pz$ pour un $z \in M$, et de $p(x-(g-1)^{p-2}z) = 0$, il résulte que $x - (g-1)^{p-2}z \in pM$ car $M(p) = pM$ vu que M est A -libre. Puisque $pM = N_1 \oplus N_{p-1}$, $(g-1)^{p-1}$ annule pM , donc aussi $(g-1)^{p-2}z$ vu que $(g-1)^{p-1}x = 0$. Alors, par le même calcul que ci-dessus et le fait que $p \geq 3$: $0 = (g-1)^{p-1}(g-1)^{p-2}z = (g-1)^{p-2} \left(\left(\sum_{k=0}^{p-1} g^k \right) z - \sum_{k=0}^{p-2} \binom{p}{k+1} (g-1)^k z \right) = - (g-1)^{p-2}pz$ car si $s \geq p-1$, $(g-1)^s pz = 0$. Finalement $px = (g-1)^{p-2}pz = 0$.

2ème cas : $r > 2$. Supposons montré que $x \in p^k M$ où $0 \leq k \leq r-2$. Alors le 1er cas s'applique à $M' = p^{r-2}M$, $L' = p^{r-2}L$ et $x' = p^{r-k-2}x$. En effet : M' est A/p^2A -libre, $pM' = p^{r-1}M$, $x' \in p^{r-k-2}pM = p^{r-2}M = M'$, $px' \in L \cap p^{r-1}M = L \cap M(p) = L(p) = p^{r-2}L = L'$, l'égalité $L(p) = p^{r-2}L$ provenant du fait que L est $A/p^{r-1}A$ -libre.

Donc par le premier cas, $px' = 0$ et $x \in M(p^{r-k-1}) = p^{k+1}M$. Ainsi, par récurrence sur k , on a finalement $x \in p^{r-1}M$, i.e. $px = 0$. $\square$

Un AG -module de type 1 typique est $A[X]/(X-1) = A$ avec action triviale de C_p . Nous désignerons ce module par A_0 pour bien indiquer qu'on le considère comme AC_p -module. De même $K_0 = K[X]/(X-1)$.

Un AC_p -module de type $p-1$ typique est $M = A[X]/(\sum_{k=0}^{p-1} X^k)$. En effet $M/pM \cong \sum_{k=0}^{p-1} K[X^k] = K[X]/(X-1)^{p-1}$ car $\sum X^k = (X^p-1)/(X-1) = (X-1)^{p-1}$.

Lemme 4.21 : $M = A[X]/(\sum_{k=0}^{p-1} X^k)$ est isomorphe à l'idéal d'augmentation de AC_p .

Preuve : L'idéal d'augmentation I est engendré par $g-1$. On considère alors :

ϕ : $AC_p \rightarrow I$ défini par $\phi(1) = g-1$. $\sum_{k=0}^{p-1} g^k \in \text{Ker } \phi$ car $(\sum g^k)(g-1) = g^p - 1 = 0$. De plus $AC_p/(\sum g^k) \cong A[X]/(\sum X^k)$. ϕ induit donc un isomorphisme $A[X]/(\sum X^k) \xrightarrow{\sim} I$ car les deux modules sont A -libres de même rang $p-1$. $\square$

On désignera par $I(A)$ l'idéal d'augmentation de AC_p , $I(K)$ celui de KC_p , etc. Dans ces nouvelles notations, un AC_p -module M est de type 1 si $M/pM \cong K_0^n$ pour un certain n , et de type $p-1$ si $M/pM \cong I(K)^n$ pour un certain n .

Théorème 4.22 : Soit M un AC_p -module A -libre de type fini, p étant impair et $r \geq 2$. Alors $M = M_1 \oplus M_{p-1} \oplus M_p$ où M_k est de type k ($k = 1, p-1, p$). De plus $pM_1 \cong (A/p^{r-1}A)_0^n$, $pM_{p-1} \cong (I(A/p^{r-1}A))^m$, où $m, n \in \mathbb{N}$, et M_p est libre.

Remarque : L'assertion sur pM_1 est équivalente à $(g-1)pM_1 = 0$ ou encore à $(g-1)M_1 \subset p^{r-1}M_1$. De même, l'assertion sur pM_{p-1} est équivalente à $(\sum_{k=0}^{p-1} g^k)M_{p-1} \subset p^{r-1}M_{p-1}$. Or ces deux inclusions sont des cas particuliers de la proposition 4.16, dès le moment où l'on sait que M_1 et M_{p-1} existent.

Preuve : L'existence du facteur libre M_p résulte de la proposition 4.13 et comme $r \geq 2$, on peut donc supposer que $p^{r-1}M \cong K_0^n \oplus I(K)^m$ pour certains entiers positifs m et n , en vertu du corollaire 4.10. Sous cette hypothèse, on peut réintroduire le cas $r = 1$ et on démontre alors l'existence de M_1 et M_{p-1} par récurrence sur $r \geq 1$. Il n'y a rien à montrer si $r = 1$.

Si $r > 1$, l'hypothèse de récurrence s'applique à pM et on a donc : $pM = C \oplus D$ avec C de type 1 et D de type $p-1$. De plus $pC \cong (A/p^{r-2}A)_0^n$ et $pD \cong I(A/p^{r-2}A)^m$. Il s'agit évidemment des mêmes entiers m et n que ci-dessus en vertu du théorème de Krull-Schmidt appliqué à $p^{r-1}M = p^{r-2}C \oplus p^{r-2}D$.

1. Montrons que $C \cong (A/p^{r-1}A)_0^n$ et que $D \cong I(A/p^{r-1}A)^m$.

Soit $M = P \oplus Q$ une décomposition de M comme A -module telle que $pP = C$ et $pQ = D$. Une telle décomposition existe car si $px_1, \dots, px_n$ est une $A/p^{r-1}A$ -base de C et si $py_1, \dots, py_l$ est une A/pA -base de D , alors $x_1, \dots, x_n, y_1, \dots, y_l$ est une A -base de M et on pose $P = \bigoplus Ax_i$ et $Q = \bigoplus Ay_j$.

a) Soit $x \in P$. $(g-1)p^{r-1}x = 0$ car $p^{r-1}x \in p^{r-2}C \cong K_0^n$ et C_p agit trivialement

sur K_0^n . Donc $(g-1)x \in M(p^{r-1}) = pM$. $(g-1)x = c + d$, $c \in C$, $d \in D$. Il résulte de $0 = (\sum_0^{p-1} g^k)(g-1)x = (\sum g^k)c + (\sum g^k)d$ que $(\sum g^k)c = 0$. Alors : $0 = (\sum g^k)c = \sum_0^{p-1} \binom{p}{k+1} (g-1)^k c = pc + (g-1)^{p-1}c$ en vertu du lemme 4.19 puis du fait que g agit trivialement sur pC , ce qui implique $(g-1)^k \binom{p}{k+1} c = 0$, $1 \leq k \leq p-2$. Maintenant $(g-1)c \in pC$ car C est de type 1 et donc $(g-1)^2 c = 0$. Comme $p \geq 3$, $(g-1)^{p-1}c = 0$ et donc finalement $pc = 0$. Alors $(g-1)px = pd$ et vu que $(g-1)px \in C$ car $px \in C$ et C est sous-module, on a $(g-1)px \in C \cap D = 0$. Ceci montre que C_p agit trivialement sur $pP = C$ et donc $C \cong (A/p^{r-1}A)_0^n$.

b) Soit maintenant $y \in Q$. $(\sum_0^{p-1} g^k)p^{r-1}y = 0$ car $p^{r-1}y \in p^{r-2}D \cong I(K)^m$ et $\sum g^k$ annule $I(K)$. Donc $(\sum g^k)y \in pM$. $(\sum g^k)y = c + d$, $c \in C$, $d \in D$. Il résulte de $0 = (g-1)(\sum g^k)y = (g-1)c + (g-1)d$ que $(g-1)c = (g-1)d = 0$. Par le lemme 4.20 appliqué à pM et au sous-module pD de p^2M , on a $pd = 0$. Alors $(\sum g^k)py = pc$ et vu que $(\sum g^k)py \in D$ car $py \in D$ et D est un sous-module, on a $(\sum g^k)py \in C \cap D = 0$. Ceci montre que $\sum g^k$ annule $D = pQ$. Mais $p^{r-2}D \cong (K[X]/(\sum X^k))^m$ et si $p^{r-2}z_1, \dots, p^{r-2}z_m$ est une base de $p^{r-2}D$, comme $K[X]/(\sum X^k)$ -module, alors $z_1, \dots, z_m$ est une base de D comme $(A/p^{r-1}A)[X]/(\sum X^k)$ -module (cf. lemme 4.15). Donc $D \cong I(A/p^{r-1}A)^m$.

2. $pM = p \cdot \text{Ker}(g-1)^{p-1} \oplus (g-1)^{p-1}M \cong p \text{Ker}(g-1)^{p-1} \cong C$, $(g-1)^{p-1}M \cong D$.

Soit $\phi: pM \rightarrow pM$ défini par $\phi(px) = (g-1)^{p-1}x$. $(g-1)^{p-1}x \in pM$ car $(g-1)^{p-1}$ annule $M/pM \cong p^{r-1}M \cong K_0^n \oplus I(K)^m$. ϕ est bien défini car si $px = 0$, $x \in p^{r-1}M$ et $(g-1)^{p-1}x = 0$. On a donc une suite exacte :

$$0 \rightarrow p \text{Ker}(g-1)^{p-1} \rightarrow pM \xrightarrow[\text{S}]{\phi} (g-1)^{p-1}M \rightarrow 0 \quad \text{où } s \text{ est l'injection de } (g-1)^{p-1}M \text{ dans } pM.$$

s n'est pas une section de ϕ mais permettra d'en construire une.

a) $\phi|_D: D \rightarrow (g-1)^{p-1}M$ est un isomorphisme. En effet, si $px \in D$ et $(g-1)^{p-1}x = 0$, alors $px = 0$ par le lemme 4.20, ce qui montre que $\phi|_D$ est injective.

On considère à nouveau la décomposition $M = P \oplus Q$ comme A -module où $pP = C$ et $pQ = D$. Alors $\text{Im} \phi|_D = (g-1)^{p-1}Q \subset (g-1)^{p-1}M$ et pour montrer l'égalité, il suffit de montrer que $(g-1)^{p-1}P \subset (g-1)^{p-1}Q$. Ainsi $\phi|_D$ sera surjective. Soit donc $x \in P$. $(g-1)x \in pM$ comme dans 1.a), et il suffit de montrer que $(g-1)^{p-2}pM \subset (g-1)^{p-1}Q$. Or $pM = C \oplus D$ et g agit trivialement sur C par 1.a).

Comme $p \geq 3$, $(g-1)^{p-2}C = 0$ et $(g-1)^{p-2}pM = (g-1)^{p-2}D$. Alors :
 $(g-1)^{p-2}(g-1)^{p-1}Q \subset (g-1)^{p-2}pM = (g-1)^{p-2}D \xrightarrow{\phi} (g-1)^{p-2}(g-1)^{p-1}Q$. La composée
 est injective, donc surjective car $(g-1)^{2p-3}Q$ est artinien. En particulier, la
 première inclusion est une égalité et $(g-1)^{p-2}pM = (g-1)^{2p-3}Q \subset (g-1)^{p-1}Q$,
 cette dernière inclusion provenant du fait que $(g-1)^{p-1}Q = \text{Im}(\phi|_D)$ est un sous-
 module.

b) $\phi \circ s$ est injective. En effet si $x \in (g-1)^{p-1}M$ alors $x = py$ pour un $y \in M$.
 Si $\phi(x) = 0$, $(g-1)^{p-1}y = 0$. Le lemme 4.20 s'applique au sous-module
 $(g-1)^{p-1}M$ de pM car il est isomorphe à D , donc de type $p-1$ et $A/p^{r-1}A$ -libre.
 On a donc $x = py = 0$. Ceci montre en fait que $p\text{Ker}(g-1)^{p-1} \cap (g-1)^{p-1}M = 0$.
 $\phi \circ s : (g-1)^{p-1}M \rightarrow (g-1)^{p-1}M$ étant injective et $(g-1)^{p-1}M$ étant artinien,
 $\phi \circ s$ est un automorphisme de $(g-1)^{p-1}M$ et par conséquent $t = s \circ (\phi \circ s)^{-1}$
 est une section de ϕ . Alors $pM = p\text{Ker}(g-1)^{p-1} \oplus t(g-1)^{p-1}M = p\text{Ker}(g-1)^{p-1} \oplus$
 $\oplus (g-1)^{p-1}M$. Comme $(g-1)^{p-1}M \cong D$, $p\text{Ker}(g-1)^{p-1} \cong C$ par le théorème de Krull-
 Schmidt.

3. Construction de M_1 et M_{p-1} .

Au point 2, on a modifié la décomposition de pM et on pose donc maintenant
 $C = p\text{Ker}(g-1)^{p-1}$ et $D = (g-1)^{p-1}M$.

a) $D \cong I(A/p^{r-1}A)^m \cong B^m$ où $B = (A/p^{r-1}A)[X]/(\sum_0^{p-1} X^k)$. A noter que B est un
 anneau court d'uniformisante $X-1$, extension totalement ramifiée de degré $p-1$
 de $A/p^{r-1}A$, en vertu de l'exemple 1.12. Soit $\{px_1, \dots, px_m\}$ une base de D
 comme B -module, où les x_i appartiennent à M . Comme les $(g-1)^s px_i$ ($1 \leq i \leq m$,
 $0 \leq s \leq p-2$) forment une $A/p^{r-1}A$ -base de D , les $(g-1)^s x_i$ ($1 \leq i \leq m$,
 $0 \leq s \leq p-2$) engendrent un sous- A -module A -libre M_{p-1} de M tel que $pM_{p-1} = D$. M_{p-1} est
 invariant par C_p car si $s < p-2$, $(g-1)(g-1)^s x_i = (g-1)^{s+1} x_i \in M_{p-1}$ et pour
 $s = p-2$, $(g-1)(g-1)^{p-2} x_i = (g-1)^{p-1} x_i$ appartient à $(g-1)^{p-1}M = D \subset M_{p-1}$.

b) $C \cong (A/p^{r-1}A)_0^n$. Soit $\{py_1, \dots, py_n\}$ une base de C comme $A/p^{r-1}A$ -module,
 où les y_j appartiennent à $\text{Ker}(g-1)^{p-1}$. Comme $(g-1)py_j = 0$, $(g-1)y_j \in p^{r-1}M =$
 $= p^{r-2}C \oplus p^{r-2}D$. $(g-1)y_j = p^{r-2}c_j + p^{r-2}d_j$. Comme $y_j \in \text{Ker}(g-1)^{p-1}$ et
 $(g-1)c_j = 0$, $(g-1)^{p-2}p^{r-2}d_j = 0$. Mais $p^{r-2}D = (K[X]/(\sum_0^{p-1} X^k))^m = (K[X]/(X-1)^{p-1})^m$
 et donc $(p^{r-2}D)((g-1)^{p-2}) = (g-1)p^{r-2}D$. Ainsi $p^{r-2}d_j = (g-1)p^{r-2}d'_j$. Posons
 alors $z_j = y_j - p^{r-2}d'_j$. On a $pz_j = py_j$ et par conséquent les z_j ($j=1, \dots, n$)
 engendrent un sous- A -module A -libre M_1 de M tel que $pM_1 = C$. M_1 est invariant

par C_p car $(g-1)z_j = (g-1)y_j - (g-1)p^{r-2}d'_j = p^{r-2}c_j$ et $C \subset M_1$.

Comme les $(g-1)^s p x_i$ et les $p z_j$ forment une $A/p^{r-1}A$ -base de $C \oplus D = pM$, les $(g-1)^s x_i$ et les z_j forment une A -base de M et ceci montre que $M = M_1 \oplus M_{p-1}$. Les assertions sur $pM_1 = C$ et $pM_2 = D$ ont été montrées sous 1. $\square$

Remarques : 1) Comme $(g-1)M_1 \subset C$ et que $(g-1)C = 0$, il s'avère que $(g-1)^2 M_1 = 0$ et donc que $C = p\text{Ker}(g-1)^{p-1} = p\text{Ker}(g-1)^2$.

2) Le théorème donne une méthode explicite de décomposition en types d'un AC_p -module A -libre M . On extrait d'abord le facteur libre (type p) en relevant une base du facteur libre de M/pM . Si on désigne encore par M le module restant, on calcule $(g-1)^{p-1}M$ et, en fonction de la remarque 1, $p\text{Ker}(g-1)^2$. On obtient ainsi une décomposition de pM qu'on relève en une décomposition de M comme dans le point 3 de la preuve du théorème.

Corollaire 4.23 : Soit M un AC_p -module A -libre de type fini, p étant impair.

(1) M est de type 1 si et seulement si $(g-1)^2 M = 0$.

(2) M est de type $p-1$ si et seulement si $(g-1)^{p-1} M = pM$.

Preuve : En vertu du théorème, il est clair que si M est de type 1 (respectivement $p-1$), alors $(g-1)^2 M = 0$ (respectivement $(g-1)^{p-1} M = pM$). Pour la réciproque, on décompose $M = M_1 \oplus M_{p-1} \oplus M_p$, M_k de type k . Si $(g-1)^2 M = 0$, alors $(g-1)^2 M_{p-1} = (g-1)^2 M_p = 0$, ce qui n'est possible que si $M_{p-1} = M_p = 0$, car sinon k doit être le plus petit entier tel que $(g-1)^k M_k \subset pM_k$.

Si maintenant $(g-1)^{p-1} M = pM$, alors $pM_1 = (g-1)^{p-1} M_1 \subset (g-1)^2 M_1 = 0$ et donc $M_1 = 0$. De plus $(g-1)^{p-1} M_p \subset pM_p$ si $M_p \neq 0$. $\square$

Comme annoncé, voici deux exemples de modules qui ne se décomposent pas en types (lorsque $s \geq 2$).

Exemples : 1) On prend $s \geq r \geq 2$, ce qui implique que $(X-1)^p | X^{p^s-1}$ (proposition 4.2). On définit M comme étant A -libre de base x, y, z , l'action de g étant donnée par : $(g-1)x = p^{r-1}y$, $(g-1)y = z$, $(g-1)z = p^{r-1}x$. On vérifie aisément que $(g-1)^3 M = 0$, et comme $(g-1)^3 | g^{p^s-1}$, M est bien un AC -module. $M/p^{r-1}M$, et a fortiori M/pM , est somme directe d'un module de type 1 et d'un module de type 2.

Montrons que M est néanmoins indécomposable :

Si $\phi \in \text{End}_{\text{AG}} M$, un calcul facile, exprimant le fait que ϕ commute à g , montre que la matrice de ϕ dans la base x, y, z est de la forme

$$\phi = \begin{pmatrix} a & c + pd & p^{r-1}b \\ p^{r-1}b & a + pe & p^{r-1}c \\ c & b + pf & a + pe \end{pmatrix}.$$

On veut montrer que $\text{End}_{\text{AG}} M$ est local. En vertu de la proposition 2.3, il suffit de montrer que l'image E de $\text{End}_{\text{AG}} M \rightarrow \text{End}_{\text{KG}} M/pM$ est un anneau local.

$$\text{Or } E \cong \left\{ \begin{pmatrix} a & c & 0 \\ 0 & a & 0 \\ c & b & a \end{pmatrix} \mid a, b, c \in K \right\} \subset M_3(K).$$

Si $\phi \in E$, ϕ est inversible $\Leftrightarrow a \neq 0$. L'ensemble des non-inversibles de E forme donc un idéal et E est local.

2) $s \geq 2$, $r \geq 2$. On définit M par $(g^{p-1})x = p^{r-1}y$, $(g-1)y = 0$, $\{x, gx, \dots, g^{p-1}x, y\}$ étant une A -base de M . $(g^{p^2-1})x = (\sum_{k=0}^{p-1} g^{kp})p^{r-1}y = p \cdot p^{r-1}y = 0$, ce qui montre que M est bien un AG -module. $M/p^{r-1}M$, et a fortiori M/pM , est clairement somme directe d'un module de type p et d'un module de type 1.

Si M était décomposable, il devrait être somme directe d'un module N de type p et d'un module N' de type 1. Montrons que c'est impossible.

a) Si $\exists z \in N$, $z = \sum_{i=0}^{p-1} a_i g^i x + by$, tel que $\sum a_i \notin pA$, alors $p^{r-1}y \in N$. En effet $(g^{p-1})g^i x = p^{r-1}y$, $\forall i = 0, \dots, p-1$, donc $(g^{p-1})z = \sum a_i p^{r-1}y$, et $\sum a_i$ est inversible par hypothèse. Comme N est A -libre, $p^{r-1}y \in N \cap M(p) = N(p) = p^{r-1}N$. Mais $p^{r-1}N \cong K[X]/(X-1)^p$ car N est de type p , et comme $(g-1)p^{r-1}y = 0$, il existe $p^{r-1}y' \in p^{r-1}N$ tel que $(g-1)p^{r-1}y' = p^{r-1}y$. Ceci est impossible car $(g-1)p^{r-1}y'$ est de rang 1 sur K engendré par $(g-1)p^{r-1}x$.

b) On suppose maintenant que $\forall z \in N$, $z = \sum_{i=0}^{p-1} a_i g^i x + by$, alors $\sum a_i \in pA$. Comme $g^p x \equiv x \pmod{p^{r-1}}$ et que $\sum_{k=0}^{p-1} g^k y = py$, on a : $\sum_{k=0}^{p-1} g^k z \equiv \sum_{i=0}^{p-1} a_i \sum_{k=0}^{p-1} g^{k+i} x \equiv (\sum_{i=0}^{p-1} a_i) (\sum_{k=0}^{p-1} g^k x) \equiv 0 \pmod{p}$. Il en résulte que $(\sum_{k=0}^{p-1} g^k)N \subset pN$ et donc que N est de type $\leq p-1$, ce qui est contradictoire.

56 Classification des AC_p -modules

Il résulte du théorème 4.22 qu'un AC_p -module A -libre indécomposable est du type 1, du type $p-1$ ou du type p .

Type p Un module du type p est projectif en vertu de la proposition 4.13, donc libre car AC_p est local (d'idéal maximal engendré par p et $g-1$). Il n'y a donc qu'un seul indécomposable, le module libre de rang 1.

Type 1 La classification est donnée par le théorème 4.17. Si M est de type 1, on a $(g-1)M \subset p^{r-1}M$ et l'endomorphisme caractéristique de M est ϕ : $p^{r-1}M \rightarrow p^{r-1}M$, $\phi(p^{r-1}x) = (g-1)x$. L'anneau B du théorème 4.17 n'est autre que K , et par conséquent $p^{r-1}M$ est un $K[Y]$ -module, Y agissant par ϕ . La condition $RY = 0$ du théorème 4.17 est toujours satisfaite comme on l'a vu dans l'exemple 1 suivant ce théorème. Comme $p^{r-1}M$ est de dimension finie sur K , c'est un $K[Y]$ -module de type fini de torsion, et la classification des modules de type 1 se réduit à celle des $K[Y]$ -modules de torsion. Mais cette dernière est bien connue car $K[Y]$ est un anneau principal : un $K[Y]$ -module de type fini de torsion indécomposable est de la forme $\bar{M} = K[Y]/(f)$ où f est une puissance d'un polynôme irréductible sur K (qu'on choisit unitaire).

Si $f = \sum_{i=0}^n a_i Y^i$ avec $a_n = 1$, l'endomorphisme ϕ de multiplication par Y est défini sur la base $\{1, Y, \dots, Y^{n-1}\}$ de $\bar{M}$ par $\phi(Y^i) = Y^{i+1}$ si $0 \leq i \leq n-2$ et $\phi(Y^{n-1}) = -\sum_{i=0}^{n-1} a_i Y^i$. Le module M de type 1 indécomposable correspondant à $\bar{M}$ admet par conséquent une A -base $\{x_0, \dots, x_{n-1}\}$ sur laquelle l'action de g est définie par $gx_i = x_i + p^{r-1}x_{i+1}$ si $0 \leq i \leq n-2$ et $gx_{n-1} = x_{n-1} - \sum_{i=0}^{n-1} p^{r-1}a_i x_i$, où $a_i \in A$ a pour image a_i dans $A/pA = K$. $p^{r-1}a_i$ est indépendant du choix du relevé a_i de a_i . M admet donc la présentation suivante :

$$M = \langle x_0, \dots, x_{n-1} \mid (g-1)x_i = p^{r-1}x_{i+1} \ (i=0, \dots, n-2), (g-1)x_{n-1} = -\sum_{i=0}^{n-1} p^{r-1}a_i x_i \rangle$$

Comme le degré d'une puissance d'un polynôme irréductible peut être aussi grand qu'on veut, on voit qu'il existe des modules de type 1 indécomposables de rang arbitrairement grand.

L'assertion (3) du théorème 4.17 peut s'exprimer de la façon suivante :

Si M est de type 1, alors M est un AC_p -module irréductible si et seulement si $p^{r-1}M$ est un $K[Y]$ -module simple. En effet, un $K[Y]$ -module irréductible n'admet par définition aucun sous-module K -libre propre et non nul, mais

comme K est un corps, cela revient à dire qu'il est simple. Par ailleurs, M est irréductible comme module de type 1 si et seulement si il l'est comme $A_{\mathbb{P}}$ -module. On a en effet :

Lemme 4.24 : Tous sous-module A -libre d'un module de type 1 est de type 1.

Preuve : Un module M de type 1 est caractérisé par le fait que $(g-1)^2 M = 0$, en vertu du corollaire 4.23. Cette condition est évidemment héritée par les sous-modules de M . $\square$

Un $K[Y]$ -module simple est de la forme $K[Y]/(f)$ où f est irréductible. S'il existe des polynômes irréductibles de degré aussi grand qu'on veut (par exemple si $K = \mathbb{F}_p$), alors il existe des modules de type 1 irréductibles de rang arbitrairement grand. Remarquons aussi que comme il existe toujours une infinité de polynômes irréductibles sur K , il existe une infinité de modules irréductibles non isomorphes.

Type $p-1$ Plusieurs méthodes permettent de classer les modules de type $p-1$.

a) La première est une conséquence directe de la proposition 4.14 : le complément N d'un module M de type 1 est de type $p-1$ et tout module de type $p-1$ est le complément d'un module de type 1. De plus M est indécomposable si et seulement si N l'est. On obtient donc la liste complète des modules de type $p-1$ indécomposables en prenant les compléments des modules de type 1 indécomposables.

Si $M = \langle x_0, \dots, x_{n-1} \mid (g-1)x_1 = p^{r-1}x_{1+1} \ (i = 0, \dots, n-2), (g-1)x_{n-1} = -\sum_{i=0}^{n-1} p^{r-1}a_i x_i \rangle$, le module libre L de base $x_0, \dots, x_{n-1}$ est la couverture projective de M car $L/pL = (K[X]/(X-1)^p)^n$ est la couverture projective de $M/pM \cong K^n$. Il en résulte que N est le sous-module de L engendré par $y_i = (g-1)x_i - p^{r-1}x_{i+1} \ (i = 0, \dots, n-2), y_{n-1} = (g-1)x_{n-1} + \sum_{i=0}^{n-1} p^{r-1}a_i x_i$. Les y_i satisfont les relations :

$(\sum_{k=0}^{p-1} g^k)y_1 = -(\sum_{k=0}^{p-1} g^k)p^{r-1}x_{1+1} = -(g-1)^{p-1}p^{r-1}x_{1+1} = -(g-1)^{p-2}p^{r-1}y_{1+1} \ (i = 0, \dots, n-2)$
et de même $(\sum_{k=0}^{p-1} g^k)y_{n-1} = \sum_{i=0}^{n-1} (g-1)^{p-2}p^{r-1}a_i y_i$.

Alors $N = \langle y_0, \dots, y_{n-1} \mid (\sum_{k=0}^{p-1} g^k)y_i = -(g-1)^{p-2}p^{r-1}y_{i+1} \ (i = 0, \dots, n-2), (\sum_{k=0}^{p-1} g^k)y_{n-1} = \sum_{i=0}^{n-1} (g-1)^{p-2}p^{r-1}a_i y_i \rangle$ car les deux modules sont A -libres de même rang $n(p-1)$, comme on le voit par réduction modulo p .

b) La deuxième méthode résulte de la classification des modules de type k (théorème 4.17). Dans les notations de ce théorème, on a $Q = \sum_{k=0}^{p-1} X^k$, $e = r-1$, $B = K[X]/(Q) = K[X]/(X-1)^{p-1}$, $R = X-1$. Si M est un module de type $p-1$, $p^{r-1}M$ est un $B[Y]$ -module B -libre de rang n qui doit satisfaire $(X-1)Yp^{r-1}M = 0$. Cela signifie que $(X-1)p^{r-1}M \subset \text{Ker } Y$ et $\text{Im } Y \subset (X-1)p^{r-2}p^{r-1}M$ car B est un anneau court de longueur $p-1$ et d'uniformisante $X-1$.

Via l'isomorphisme $(X-1)p^{r-2}p^{r-1}M \cong p^{r-1}M/(X-1)p^{r-1}M$, Y induit un endomorphisme Y de $\bar{M} = p^{r-1}M/(X-1)p^{r-1}M = K^n$. Comme dans le cas des modules de type 1, on est réduit à classer les $K[Y]$ -modules de type fini de torsion.

Si $\bar{M} = K[Y]/(f)$ où f est une puissance d'un polynôme irréductible sur K et si $f = \sum_{i=0}^n a_i Y^i$ avec $a_n = 1$, alors en remontant au B -module libre $p^{r-1}M$, Y est défini sur une base $p^{r-1}x_0, \dots, p^{r-1}x_{n-1}$ par $Y(p^{r-1}x_i) = (X-1)p^{r-2}p^{r-1}x_{i+1}$ ($i = 0, \dots, n-2$) et $Y(p^{r-1}x_{n-1}) = -\sum_{i=0}^{n-1} (X-1)p^{r-2}p^{r-1}a_i x_i$, où $a_i \in A$ a pour image a_i dans K . Comme $Y(p^{r-1}x) = Qx$ par définition de l'endomorphisme caractéristique de M , on en déduit que M admet la présentation suivante :

$$M = \langle x_0, \dots, x_{n-1} \mid (\sum g^k) x_i = (g-1)p^{r-2}p^{r-1}x_{i+1} \quad (i = 0, \dots, n-2), (\sum g^k) x_{n-1} = \sum_{i=0}^{n-1} (g-1)p^{r-2}p^{r-1}a_i x_i \rangle.$$

On retrouve aux signes près la même présentation que celle obtenue par la première méthode, ce qui prouve en fait que si ϕ est l'endomorphisme caractéristique d'un module M de type 1, alors $-\phi$ est l'endomorphisme caractéristique du complément N de M , considéré comme endomorphisme du K -espace vectoriel $\bar{N} = p^{r-1}N/(g-1)p^{r-1}N \cong (g-1)p^{r-2}p^{r-1}N$ qui est de même dimension que $p^{r-1}M$.

c) Signalons encore le point de vue de Hannula [Ha 1]. Il montre que le produit tensoriel par l'idéal d'augmentation $I(A)$ de AC_p induit une bijection de l'ensemble des classes d'isomorphisme de modules de type 1 sur l'ensemble des classes d'isomorphisme de modules de type $p-1$ et que cette bijection préserve les indécomposables.

Cela résulte de la proposition 4.14 car on a en fait :

Proposition 4.25 : Soit M un module de type 1. Alors $I(A) \otimes_A M$ est le complément de M .

Preuve : On a une suite exacte $0 \rightarrow I(A) \rightarrow AC_p \rightarrow A \rightarrow 0$, qui donne après tensorisation par $M : 0 \rightarrow I(A) \otimes_A M \rightarrow AC_p \otimes_A M \rightarrow M \rightarrow 0$.

On a vu que si M est A -libre de rang n , alors la couverture projective de M est AC_p -libre de rang n . Il suffit donc de vérifier que $AC_p \otimes_A M$ est AC_p -libre de rang n . Or ceci n'est autre qu'un résultat classique de Frobenius :

si M_0 désigne le A -module M avec action triviale de C_p , on a un isomorphisme $\phi : AC_p \otimes_A M_0 \rightarrow AC_p \otimes_A M$ défini par $\phi(x \otimes m) = x \otimes xm$.
Or $AC_p \otimes_A M_0 \cong (AC_p)^n$. $\square$

Soit $L_A(G)$ le quotient du groupe abélien libre engendré par les classes d'isomorphisme $[M]$ de AG -modules A -libres de type fini par le sous-groupe engendré par les éléments de la forme $[M \oplus M'] - [M] - [M']$. En vertu du théorème de Krull-Schmidt, $L_A(G)$ est abélien libre engendré par les classes d'isomorphisme de modules indécomposables. Le produit tensoriel de représentations induit une structure d'anneau sur $L_A(G)$, d'unité la classe du module trivial A . La classification des indécomposables dans le cas $G = C_p$ détermine entièrement la structure additive de $L_A(G)$. La structure multiplicative a été étudiée par Hannula [Ha 1 et 2] et ses résultats sont les suivants :

(1) $[AC_p] \cdot [M] = n [AC_p]$ où n est le rang de M .

On a en effet : $AC_p \otimes_A M = AC_p \otimes_A M_0 \cong (AC_p)^n$, comme dans la proposition 4.25.

(2) $[I(A)]^2 = (p-2)[AC_p] + [A]$.

En posant $I = I(A)$ et $L = AC_p$, on a : $0 \rightarrow I \rightarrow L \rightarrow A \rightarrow 0$, donc $0 \rightarrow I \otimes I \rightarrow L^{p-1} \xrightarrow{f} I \rightarrow 0$ car $L \otimes I \cong L^{p-1}$ en vertu de (1).

Or L est la couverture projective de I et on a une suite exacte

$0 \rightarrow A \rightarrow L \rightarrow I \rightarrow 0$ car $I \cong AC_p / (\sum g^k)$. Donc $L^{p-1} \xrightarrow{f} I$ se factorise par L et il vient :

$$\begin{array}{ccccccc} 0 & \rightarrow & I \otimes I & \rightarrow & L^{p-1} & \xrightarrow{f} & I \rightarrow 0 \\ & & \downarrow g & & \downarrow h & & \parallel \\ 0 & \rightarrow & A & \rightarrow & L & \rightarrow & I \rightarrow 0 \end{array}$$

Ainsi $\text{Ker} h = L^{p-2} \subset \text{Ker} f$ et donc $I \otimes I \cong L^{p-2} \oplus M$ pour un certain M , car L^{p-2} est injectif.

Comme $L^{p-2} \subset \text{Ker} g$, g induit $\tilde{g} : M \rightarrow A$. Mais M est de rang 1 car $I \otimes I$ est de rang $(p-1)^2 = p(p-2)+1$, et donc $\tilde{g}$ est un isomorphisme.

La formule en résulte.

(3) En vertu de la proposition 4.25, il ne reste plus qu'à déterminer le produit tensoriel de deux modules de type 1. En effet le produit tensoriel de deux modules de type $p-1$ est donné par $[I \otimes M] \cdot [I \otimes N] = [I]^2 \cdot [M] \cdot [N] = [M] \cdot [N] + mn(p-2)[\bar{A}C_p]$, où M et N sont de type 1, de rang m et n respectivement.

Le produit tensoriel de deux modules de type 1 M et M' est encore de type 1 car g agit par l'identité modulo p sur M et M' , donc aussi sur $M \otimes_A M'$.

De plus, on a un isomorphisme $\phi: p^{r-1}(M \otimes_A M') \rightarrow p^{r-1}M \otimes_K p^{r-1}M'$ donné par $\phi(p^{r-1}(x \otimes y)) = p^{r-1}x \otimes p^{r-1}y$. $p^{r-1}M$, $p^{r-1}M'$ et $p^{r-1}(M \otimes_A M')$ sont des $K[Y]$ -modules, Y agissant par leur endomorphisme caractéristique. En transportant par ϕ la structure de $K[Y]$ -module de $p^{r-1}(M \otimes_A M')$, on voit que Y agit par $Y \otimes 1$ et $1 \otimes Y$ sur $p^{r-1}M \otimes_K p^{r-1}M'$. En effet : $Y p^{r-1}(x \otimes y) = (g-1)(x \otimes y) = (g-1)x \otimes (g-1)y + x \otimes (g-1)y = (g-1)x \otimes y + x \otimes (g-1)y$, car $(g-1)x \in p^{r-1}M$, $(g-1)y \in p^{r-1}M'$ et $p^{r-1} \cdot p^{r-1} = 0$, et en transportant par ϕ : $Y(p^{r-1}x \otimes p^{r-1}y) = (g-1)x \otimes p^{r-1}y + p^{r-1}x \otimes (g-1)y = (Y \otimes 1 + 1 \otimes Y)(p^{r-1}x \otimes p^{r-1}y)$.

Il en résulte qu'il suffit de déterminer la décomposition de $Y \otimes_K N'$ en indécomposables, N et N' étant deux $K[Y]$ -modules et Y agissant par $Y \otimes 1 + 1 \otimes Y$ sur $N \otimes_K N'$. On peut supposer N et N' indécomposables, donc la forme $N = N = K[Y]/(f^r)$ et $N' = K[Y]/(g^s)$ avec f et g irréductibles. Citons alors sans démonstration le résultat d'Hannula :

Soient A l'ensemble des zéros de f et B l'ensemble des zéros de g dans une clôture algébrique de K . Soit $\{q_1, \dots, q_m\}$ l'ensemble des polynômes minimaux des éléments $a + b$ ($a \in A$, $b \in B$) (si $a+b$ et $a'+b'$ ont même polynôme minimal q , alors q n'est compté qu'une fois). Soit $n(Y)$ le nombre de couples (a,b) ($a,b \in A \times B$) tels que $a+b = Y$. On peut montrer que $n(Y) = n(Y')$ si Y et Y' ont même polynôme minimal q_1 et on pose $n_1 = n(Y)$. Alors :

$$K[Y]/(f^r) \otimes_K K[Y]/(g^s) \cong \bigoplus_{i=1}^m \bigoplus_{j=1}^k (K[Y]/(q_1^{d_{ij}}))^{n_1}$$

où, $\forall i = 1, \dots, m$, $\{d_{i1}, \dots, d_{ik}\}$ est une famille d'entiers qui dépendent de r , de s et des degrés d'inséparabilité de f , g et q_1 . Pour plus de détails, on peut consulter [Ha 1 et 2]. Mentionnons toutefois que si f et g sont séparables et si $r = s = 1$, alors $k = 1$ et $d_{i1} = 1$, $\forall i$, si bien que

$$K[Y]/(f) \otimes_K K[Y]/(g) \cong \bigoplus_{i=1}^m (K[Y]/(q_i))^{n_1}.$$

Ceci montre en particulier que si K est parfait, le produit tensoriel de $K[Y]$ -modules semi-simples est semi-simple.

Terminons ce paragraphe en remarquant que de la classification des AC_p -modules A -libres résulte celle des DC_p -modules D -libres où D est un anneau de valuation discrète complet non ramifié de corps résiduel de caractéristique p (i.e. p est une uniformisante de D). Il s'agit d'un résultat dû à Heller-Reiner [HR] mais qu'ils obtiennent par d'autres méthodes.

Théorème 4.26 : Soit D un anneau de valuation discrète complet d'uniformisante p . Il y a, à isomorphisme près, 3 DC_p -modules indécomposables D -libres : DC_p , $D[X]/(X-1)$ et $D[X]/(\sum_{k=0}^{p-1} X^k)$.

Tout DC_p -module D -libre se décompose de manière essentiellement unique en somme directe de modules indécomposables (Krull-Schmidt).

Preuve : Soit M un DC_p -module D -libre indécomposable. En vertu du théorème 2.18, M/p^2M est indécomposable, donc aussi M/p^3M . Si M/p^3M est de type 1, $(g-1)M/p^3M \subset p^2M/p^3M$ et donc $(g-1)M/p^2M = 0$. Comme M/p^2M est indécomposable, on doit avoir $M/p^2M \cong D/p^2D$ avec action triviale de g , i.e. $M/p^2M \cong \cong (D/p^2D)[X]/(X-1)$. En vertu du point (2) du même théorème 2.18, $M \cong D[X]/(X-1)$.

Par le même raisonnement, si M/p^3M est de type $p-1$, alors $M/p^2M \cong \cong (D/p^2D)[X]/(\sum_{k=0}^{p-1} X^k)$ et donc $M \cong D[X]/(\sum_{k=0}^{p-1} X^k)$. Enfin si M/p^2M est de type p , $M/p^2M \cong (D/p^2D)C_p$ et donc $M \cong DC_p$. La préservation des indécomposables ainsi que des classes d'isomorphisme de modules par réduction modulo p^2 garantit la validité du théorème de Krull-Schmidt. $\square$

§ 7 Le groupe cyclique C_2 .

Lorsque $p = 2$, les seuls types de AC_2 -modules sont les type 1 et 2.

Les modules de type 2 sont libres et tout AC_2 -module A -libre est somme directe d'un module de type 1 et d'un module de type 2 en vertu de la proposition 4.13.

Il ne reste donc qu'à classer les modules de type 1.

On a vu que, dans le cas où p est impair, les modules M de type 1 sont caractérisés par le fait que $(g-1)M \subset p^{r-1}M$, mais ceci n'est pas valable lorsque $p = 2$ (cf. proposition 4.5). En fait, certains modules de type 1 se comportent

exactement comme les modules de type $p-1$ ($p-1 = 1$!) alors que d'autres sont d'"authentiques" modules de type 1. A cet effet, on modifie la terminologie de la manière suivante : un AC_2 -module A-libre M sera dit de type 1 si $(g-1)M \subset 2^{r-1}M$ et de type 2-1 si $(g+1)M \subset 2^{r-1}M$. Dans les deux cas on a $(g-1)M \subset M$ et $(g+1)M \subset 2M$ car $g-1 \equiv g+1 \pmod{2}$. Si $r = 2$, les deux types s'identifient et il suffit dans ce cas de classer les modules de type 1. On supposera par conséquent $r \geq 3$ dans la suite. Avec ces nouvelles conventions, le théorème 4.22 reste vrai :

Théorème 4.27 : Soit M un AC_2 -module A-libre de type fini, avec $r \geq 3$. Alors $M = M_1 \oplus M_{2-1} \oplus M_2$ où M_k est de type k ($k = 1, 2-1, 2$).

Preuve : L'existence du facteur libre M_2 résulte de la proposition 4.13 et on peut donc supposer $(g-1)M/2M = 0$.

1. Montrons que $4M = 2(g+1)M \oplus 2(g-1)M$.

Si $x \in M$, $4x = 2(g+1)x + 2(g-1)(-x)$ et donc $4M = 2(g+1)M + 2(g-1)M$.

Si $2(g+1)x = 2(g-1)y$, alors $(g+1)x - (g-1)y \in M(2) = 2^{r-1}M$, donc

$(g+1)x - (g-1)y = 2^{r-1}z = 2^{r-2}((g+1)z - (g-1)z)$ et $(g+1)(x-2^{r-2}z) = (g-1)(y-2^{r-2}z)$.

Comme $(g-1)(g+1) = g^2 - 1 = 0$, on a :

$$0 = (g+1)(g-1)(y-2^{r-2}z) - (g-1)(g+1)(x-2^{r-2}z) = ((g+1)-(g-1))(g+1)(x-2^{r-2}z) = 2(g+1)x - (g+1)2^{r-1}z = 2(g+1)x \text{ car } g+1 \text{ agit par zéro sur } 2^{r-1}M \cong M/2M.$$

Donc $2(g+1)x = 0$ ce qui montre que la somme $4M = 2(g+1)M + 2(g-1)M$ est directe.

2. Montrons que $2M = N_1 \oplus N_2$, avec $(g-1)N_1 = 0$ et $(g-1)N_2 = 0$.

Si $\{2(g-1)x_i \mid i = 1, \dots, n\}$ est une $A/2^{r-2}A$ -base de $2(g+1)M$ et si $\{2(g-1)y_j \mid j = 1, \dots, m\}$ est une $A/2^{r-2}A$ -base de $2(g-1)M$, alors les $(g+1)x_i$ ($i=1, \dots, n$) engendrent un sous-A-module N_1 de $2M$ et les $(g-1)y_j$ ($j=1, \dots, m$) un sous-A-module N_2 de $2M$ et on a $2M = N_1 \oplus N_2$.

N_1 et N_2 sont invariants par C_2 , car $(g-1)(g+1)x_i = 0$ et $(g+1)(g-1)y_j = 0$. Ceci montre aussi que $(g-1)N_1 = 0$ et $(g+1)N_2 = 0$.

3. Construction de M_1 et M_{2-1} .

Soit $\{u_1, \dots, u_n, v_1, \dots, v_m\}$ une A-base de M telle que $\{2u_1, \dots, 2u_n\}$ soit une base de N_1 et $\{2v_1, \dots, 2v_m\}$ une base de N_2 .

Comme $(g-1)2u_i = 0$ et $(g+1)2v_j = 0$, $(g-1)u_i, (g+1)v_j \in 2^{r-1}M = 2^{r-2}N_1 \oplus 2^{r-2}N_2$.
 $(g-1)u_i = 2^{r-2}(w_{i1} + w_{i2})$ et $(g+1)v_j = 2^{r-2}(z_{j1} + z_{j2})$, où $w_{ik}, z_{jk} \in N_k$ ($k=1,2$).
 Comme $r \geq 3$, $2^{r-3}w_{i2}$ et $2^{r-3}z_{j1}$ appartiennent à $2M$ et par conséquent, si
 $u'_i = u_i + 2^{r-3}w_{i2}$, $v'_j = v_j - 2^{r-3}z_{j1}$, $\{u'_1, \dots, u'_n, v'_1, \dots, v'_m\}$ est aussi une A-base de M.

On pose $M_1 = \langle u'_1, \dots, u'_n \rangle$ et $M_{2-1} = \langle v'_1, \dots, v'_m \rangle$ comme A-modules.

On a $M = M_1 \oplus M_{2-1}$, et il reste à montrer que M_1 et M_{2-1} sont invariants par C_2 .

Remarquons tout d'abord que $2^{r-1}u'_i = 2^{r-1}u_i$ et $2^{r-1}v'_j = 2^{r-1}v_j$, donc que
 $2^{r-1}M_1 = 2^{r-2}N_1$ et $2^{r-1}M_{2-1} = 2^{r-2}N_2$. Maintenant :
 $(g-1)u'_i = 2^{r-2}(w_{i1} + w_{i2}) + (g-1)2^{r-3}w_{i2}$, mais comme $w_{i2} \in N_2$ et que $(g+1)N_2 = 0$,
 on a $(g-1)w_{i2} = -2w_{i2}$ et donc $(g-1)u'_i = 2^{r-2}w_{i1}$. Il s'ensuit que
 $(g-1)M_1 \subset 2^{r-2}N_1 = 2^{r-1}M_1$ et M_1 est invariant par C_2 .

De même $(g+1)z_{j1} = 2z_{j1}$ car $(g-1)N_1 = 0$, et donc $(g+1)v'_j = 2^{r-2}(z_{j1} + z_{j2}) - 2^{r-2}z_{j1} = 2^{r-2}z_{j2}$. $(g+1)M_{2-1} \subset 2^{r-2}N_2 = 2^{r-1}M_{2-1}$ et M_{2-1} est invariant par C_2 .
 Ceci montre aussi que M_k est de type k ($k = 1, 2-1$). $\square$

La classification des AC_2 -modules A-libres se réduit donc à celle de chaque type k ($k=1, 2-1, 2$) et s'effectue exactement de la même manière que dans le cas où p est impair : le cas des modules de type 1 se ramène à celui des $K[Y]$ -modules de torsion et de même pour le type 2-1. $\sum_{k=0}^{p-1} g^k$ n'étant autre que $g+1$. Remarquons que, alors que lorsque p est impair l'endomorphisme caractéristique ϕ d'un module M de type p-1 est vu comme un endomorphisme du K-espace vectoriel $(g-1)^{p-2}p^{r-1}M$, la situation se simplifie légèrement si $p = 2$ car $(g-1)^{p-2} = 1$, g agit trivialement sur $2^{r-1}M$ et ϕ est donc un endomorphisme de $2^{r-1}M$.

Lorsque $r = 2$, les modules de type 1 et 2-1 s'identifient et la classification est réduite à celle des modules de type 1. A noter qu'on peut dans ce cas définir à choix deux endomorphismes caractéristiques d'un module M, selon qu'on considère M comme module de type 1 ou de type 2-1 :

$\phi: 2M \rightarrow 2M$, $\phi(2x) = (g-1)x$ ou bien $\phi': 2M \rightarrow 2M$, $\phi'(2x) = (g+1)x$.

Comme $(g+1)x = (g-1)x + 2x$, on a $\phi' = \phi + \text{id}$ et de même $\phi = \phi' + \text{id}$.

Proposition 4.28 : On suppose $r = 2$. Soit M un AC_p -module de type 1. Si ϕ est l'endomorphisme caractéristique de M , alors $\phi + \text{id}$ est l'endomorphisme caractéristique du complément N de M .

Preuve : Il est clair que cette proposition n'a de sens que si $2N$ et $2M$ sont identifiés par un isomorphisme canonique. Or si M est de rang n , sa couverture projective L est libre de rang n et on a une suite exacte $0 \rightarrow 2N \rightarrow 2L \xrightarrow{\pi} 2M \rightarrow 0$. On a $2L \cong [K[X]/(X-1)^2]^n$, $2M \cong [K[X]/(X-1)]^n$ et $2N \cong [(X-1)K[X]/(X-1)^2]^n$. On définit alors un isomorphisme canonique $\psi: 2M \rightarrow 2N$, $\psi(2v) = (g-1)2y$ où $u \in L$ est tel que $\pi y = v$. En fait $2L$ est un module libre sur l'anneau court $B = K[X]/(X-1)^2$ et ψ n'est autre que l'isomorphisme multiple fois rencontré $B/(X-1)B \cong (X-1)B$.

L'endomorphisme ϕ de $2M$ se relève en un endomorphisme B -linéaire ϕ de $2L$ car $2L$ est B -libre et si $\{x_1, \dots, x_n\}$ est une base de L , M admet la présentation suivante :

$$M = \langle x_1, \dots, x_n \mid (g-1)x_i - \phi(2x_i) = 0 \ (i = 1, \dots, n) \rangle$$

N est A -libre de base $y_i = (g-1)x_i = -\phi(2x_i) \ (i = 1, \dots, n)$.

Calculons l'endomorphisme caractéristique ϕ' de N :

$$\begin{aligned} \phi'(2y_i) &= (g-1)y_i = (g-1)^2 x_i - \phi((g-1)2x_i) = -2(g-1)x_i - \phi((g-1)2x_i) = \\ &= 2y_i + \phi(2y_i) \text{ car } -2=2 \text{ et } 2y_i = 2(g-1)x_i. \end{aligned}$$

Ainsi $\phi' = \phi + \text{id}$ et en transportant ϕ' sur $2M$ via l'isomorphisme ψ , on a $\psi^{-1}\phi\psi(2\bar{x}_i) = \psi^{-1}\phi(g-1)2x_i = \psi^{-1}(g-1)\phi(2x_i) = \pi\phi(2x_i) = \phi(2\bar{x}_i)$ où $\bar{x}_i = \pi x_i$, $\pi: L \rightarrow M$ étant la projection canonique. Finalement $\psi^{-1}\phi'\psi = \phi + \text{id}$. $\square$

Signalons enfin que le théorème 4.26 qui classe les OC_p -modules D -libres, où D est un anneau de valuation discrète complet d'uniformisante p , reste valable sans changement lorsque $p = 2$.

§8 Extension des scalaires.

Nous allons étudier le comportement de l'endomorphisme caractéristique d'un module de type k par extension des scalaires. A désigne toujours un p -anneau court non ramifié et $G = C_p$. Soient Q un diviseur unitaire de degré k de $X^{p^s}-1$ et M un AG -module de type k . On reprend les notations du théorème 4.17 : $s = \max(1, r-s + v_p(k))$, $B = \bar{A}[X]/(Q)$ où $\bar{A} = A/p^{r-s}A$. On suppose $r = 2$ ou $r \geq 2$ ($s - v_p(k)$). $p^s M$ est muni d'une structure de $B[Y]$ -module B -libre, où la multiplication par Y est l'endomorphisme caractéristique de M , et cette structure caractérise entièrement le module M en vertu du théorème 4.17.

Soient alors A' une extension non ramifiée de degré n de A , $\bar{A}' = A'/p^{r-s}A'$ et $B' = \bar{A}'[X]/(Q)$. Il est clair que $A' \otimes_A M$ est un $A'G$ -module de type k et par conséquent $p^s (A' \otimes_A M)$ est un $B'[Y]$ -module A' -libre, Y étant l'endomorphisme caractéristique de $A' \otimes_A M$. Par ailleurs $\bar{A}' \otimes_{\bar{A}} p^s M$ est un B' -module libre sur lequel on peut faire agir Y par $Y(a \otimes p^s x) = a \otimes Y(p^s x)$, $a \in \bar{A}'$, $x \in M$. Il s'agit en fait de l'extension des scalaires de $B[Y]$ à $B'[Y]$.

Proposition 4.29 : $p^s (A' \otimes_A M) \cong \bar{A}' \otimes_{\bar{A}} p^s M$ comme $B'[Y]$ -modules. En d'autres termes, l'extension des scalaires "commute" au passage à l'endomorphisme caractéristique.

Preuve : $p^s (A' \otimes_A M) \cong A' \otimes_A p^s M = \bar{A}' \otimes_{\bar{A}} p^s M$ comme $A'G$ -modules, donc comme B' -modules, car B' est un quotient de $A'G$ et les structures de B' -modules sont induites par celles de $A'G$ -modules. L'isomorphisme est donné par :

$$f : p^s (A' \otimes_A M) \rightarrow \bar{A}' \otimes_{\bar{A}} p^s M, f(p^s (a \otimes x)) = \bar{a} \otimes p^s x, x \in M, a \in A' \text{ et } \bar{a} = \text{classe de } a \text{ dans } \bar{A}'.$$

Reste à vérifier que f commute à Y . Or on a :

$$Y p^s (a \otimes x) = Q(a \otimes x) = a \otimes Qx = a \otimes Y p^s x, \text{ donc :}$$

$$f(Y p^s (a \otimes x)) = f(a \otimes Y p^s x) = \bar{a} \otimes Y p^s x = Y(\bar{a} \otimes p^s x) = Y f(p^s (a \otimes x)). \quad \square$$

On suppose désormais que le corps résiduel K de A est parfait de manière à ce que le treillis des extensions finies non ramifiées de A soit isomorphe par réduction modulo p au treillis des extensions finies de K (corollaire 1.19). Rappelons que si $\hat{K}$ désigne la clôture algébrique de K et $\hat{A}$ l'unique p -anneau court non ramifié de corps résiduel $\hat{K}$ (à isomorphisme près), alors le treillis des extensions finies non ramifiées de A est le treillis des sous-anneaux de $\hat{A}$ qui sont des p -anneaux courts non ramifiés (ils sont automatiquement A -libres en vertu du lemme 1.4).

$\hat{A}$ est appelé la clôture non ramifiée de A.

Il résulte du corollaire à la proposition 2.4 qu'un AG-module indécomposable est absolument indécomposable s'il reste indécomposable par extension finie (non ramifiée) des scalaires. Par analogie, on dira qu'un AG-module A-libre irréductible est absolument irréductible s'il reste irréductible par toute extension finie (non ramifiée) des scalaires. On a alors :

Proposition 4.30 : On suppose $r \geq 2s$. Les conditions suivantes sont équivalentes

- (i) Tout AG-module irréductible est absolument irréductible.
- (ii) Tout AG-module indécomposable est absolument indécomposable.
- (iii) $A = \hat{A}$.

Ainsi, contrairement au cas non-modulaire (proposition 3.13) et contrairement aussi au cas des représentations sur un corps, il n'y a en général pas d'extension finie de A qui soit anneau de décomposition de G vu qu'il faut "monter" jusqu'à la clôture non ramifiée $\hat{A}$ de A.

Preuve : Si $A = \hat{A}$, A n'admet pas d'extension non ramifiée finie et donc (iii) $\Rightarrow$ (i) et (iii) $\Rightarrow$ (ii).

On montre alors (i) $\Rightarrow$ (iii) et (ii) $\Rightarrow$ (iii) en montrant que si $A \neq \hat{A}$, alors il existe un AG-module irréductible M et une extension finie C de A telle que $C \otimes_A M$ est décomposable. On choisit M de type 1 et, en vertu de l'exemple 2 suivant le théorème 4.17, cela revient à choisir un $\bar{A}[Y]$ -module $\bar{A}$ -libre de type fini, où $\bar{A} = A/p^s A$, à savoir le module $p^s M$, $e = r-s$. Soit $\bar{f} \in \bar{A}[Y]$ tel que la réduction $\bar{f}$ modulo p de $\bar{f}$ soit irréductible sur K de degré > 1 . Un tel polynôme existe car K n'est pas algébriquement clos par hypothèse. Soit alors $N = \bar{A}[Y]/(\bar{f})$ et M le module de type 1 tel que $p^e M \cong N$ comme $\bar{A}[Y]$ -module. N est irréductible par construction et par conséquent M est irréductible comme module de type 1 par le théorème 4.17. Cela revient à dire que M est irréductible comme AG-module A-libre car tout sous-AG-module A-libre d'un module de type 1 est encore de type 1.

Relevons $\bar{f}$ en un polynôme $f \in A[Y]$ et posons $C = A[Y]/(f)$. C est extension non ramifiée de degré $n = \deg f$ de A car, K étant parfait, la réduction $\bar{f}$ modulo p de f est un polynôme irréductible séparable. On veut montrer que $C \otimes_A M$ est un CG-module décomposable. Par le théorème 4.17, il suffit de montrer que $p^e(C \otimes_A M)$ est décomposable comme $\bar{C}[Y]$ -module, où $\bar{C} = C/p^s C$. Dans les notations de la proposition 4.29, on a dans ce cas $B' = \bar{C}$ et donc $p^e(C \otimes_A M) \stackrel{\sim}{=} \bar{C} \otimes_{\bar{A}} p^e M$ comme $\bar{C}[Y]$ -modules. Tout revient donc à montrer que $\bar{C} \otimes_{\bar{A}} N \stackrel{\sim}{=} \bar{C}[Y]/(\bar{f})$ est décomposable. Or par construction $\bar{f}$ est irréductible sur le corps résiduel de $\bar{C}$: $\bar{f} = \bar{g}\bar{h}$. $\bar{g}$ et $\bar{h}$ sont premiers entre eux car $\bar{f}$ est séparable, donc par le lemme de Hensel, $\bar{g}$ et $\bar{h}$ se relèvent en des polynômes $\tilde{g}$ et $\tilde{h}$ de $\bar{C}[Y]$ tels que $\bar{f} = \tilde{g}\tilde{h}$ et de plus $(\tilde{g}, \tilde{h}) = (1)$. Il en résulte que $\bar{C}[Y]/(\bar{f}) \stackrel{\sim}{=} \bar{C}[Y]/(\tilde{g}) \oplus \bar{C}[Y]/(\tilde{h})$. $\square$

Remarques : 1) L'application répétée du théorème 4.17 semble nécessiter l'hypothèse que p est impair. En réalité, cette hypothèse n'était faite que pour garantir que $QM \subset p^e M$, à savoir $(g-1)M \subset p^{r-s}M$ dans le cas des modules de type 1. Lorsque $p = 2$, on peut redéfinir comme on l'a déjà fait au paragraphe 7 les modules de type 1 comme étant les modules M tels que $(g-1)M \subset 2^{r-s}M$. Le théorème 4.17 reste alors entièrement valable pour les modules de ce type. Par conséquent la démonstration de la proposition précédente subsiste sans changement dans le cas $p = 2$.

2) En construisant un module M de type 1 tel que $(g-1)M \subset p^{r-1}M$, on peut aisément reconduire la démonstration dans le cas $r \geq 2$ en supprimant l'hypothèse $r \geq 2s$. Cela nécessite uniquement une adaptation du théorème 4.17, qui ne pose aucun problème.

§9 Modules duaux et bicompléments

Rappelons qu'on a défini le dual d'un AG-module (à gauche) M comme étant le AG-module à droite $M^* = \text{Hom}_A(M, A)$, l'action de AG étant définie par $(fa)x = f(ax)$, $f \in M^*$, $a \in AG$, $x \in M$. Lorsque $G = C_p^s$, AG est abélien et on peut donc voir M^* comme AG-module à gauche.

Lemme 4.31 : Si M est de type k , M^* est de type k .

Preuve : Par la proposition 2.21, $M^*/pM^* \stackrel{\sim}{=} (M/pM)^*$ et il suffit de vérifier que le dual d'un KG-module de type k est de type k . Il n'y a qu'un seul KG-module indécomposable de type k : $N = K[X]/(X-1)^k$. N^* doit être indécomposable et de dimension k sur K . Or N est l'unique indécomposable de dimension k . Donc $N \stackrel{\sim}{=} N^*$. $\square$

Lemme 4.32 : a) $(M \otimes_A N)^* \cong M^* \otimes_A N^*$

b) $I^* \cong I$ où I est l'idéal d'augmentation de AC_p .

Preuve : a) Si α est la matrice de g par rapport à une base $\{x_i\}$ de M , on vérifie aisément que la transposée ${}^t\alpha$ de α est la matrice de g par rapport à la base duale $\{x_i^*\}$ de M^* . Si maintenant β est la matrice de g dans une base $\{y_j\}$ de N , alors ${}^t(\alpha \otimes \beta)$ est la matrice de g dans la base $(x_i \otimes y_j)^*$ de $(M \otimes_A N)^*$ et ${}^t\alpha \otimes {}^t\beta$ est la matrice de g dans la base $x_i^* \otimes y_j^*$ de $M^* \otimes_A N^*$. Comme ${}^t(\alpha \otimes \beta) = {}^t\alpha \otimes {}^t\beta$, cela démontre a).

b) Comme $I \cong A[x] / (\sum_{k=0}^{p-1} x^k)$, I admet une base $x_1, \dots, x_{p-1}$ sur laquelle g agit par $gx_i = x_{i+1}$ ($i < p-1$), $gx_{p-1} = -\sum_{i=1}^{p-1} x_i$. En prenant la transposée de la matrice de g dans cette base, on voit que g agit sur la base duale par :

$gx_1^* = -x_{p-1}^*$, $gx_i^* = x_i^* - x_{p-1}^*$ ($i > 1$). On pose $y_1 = x_{p-1}^*$, $y_i = x_i^* - x_{p-1}^*$ ($i > 1$) et on vérifie que $gy_i = y_{i+1}$ ($i < p-1$), $gy_{p-1} = -\sum_{i=1}^{p-1} y_i$. g a donc la même action sur les y_i que sur les x_i , ce qui montre que $I^* \cong I$. $\square$

A remarquer que b) se généralise de manière évidente au groupe cyclique C_p .

Proposition 4.33 : Tout AC_p -module A -libre de type fini est isomorphe à son dual.

Preuve : Si M est de type p , c'est-à-dire libre, M^* est aussi libre en vertu du lemme 4.31 et comme les rangs sont préservés par passage au dual, $M \cong M^*$. Si M est de type $p-1$, alors $M \cong I \otimes_A N$, où N est de type 1, par la proposition 4.25. Par le lemme 4.32, $M^* \cong I \otimes_A N^*$ et il suffit de montrer la proposition pour un module de type 1.

Si M est de type 1, $V = p^{r-1}M$ est un $K[Y]$ -module, dont on peut prendre le dual V^* comme K -espace vectoriel. Y agit sur V^* par $(Yf)(v) = f(Yv)$, $f \in V^*$, $v \in V$. Par la proposition 2.20, $p^{r-1}M^* \cong V^*$ et on veut montrer que cet isomorphisme commute à Y , Y agissant sur $p^{r-1}M^*$ par l'endomorphisme caractéristique de M^* , qui est de type 1. L'isomorphisme $\phi : p^{r-1}M^* \rightarrow V^*$ est donné par $\phi(p^{r-1}f)(p^{r-1}x) = \overline{f(x)}$, où $x \in M$, $p^{r-1}x \in p^{r-1}M = V$, et où $\overline{f(x)}$ désigne l'image dans K de $f(x) \in A$.

$Yp^{r-1}f = p^{r-1}h$ pour un certain $h \in M^*$, si $f \in M^*$. On a alors :

$(p^{r-1}h)(x) = (Yp^{r-1}f)(x) = ((g-1)f)(x) = f((g-1)x) = f(p^{r-1}y) = (p^{r-1}f)(y)$, où y est tel que $(g-1)x = p^{r-1}y$. On a donc $p^{r-1}(h(x) - f(y)) = 0$, $h(x) - f(y) \in pA$ et par conséquent $\overline{h(x)} = \overline{f(y)}$. Alors :

$\phi(\gamma p^{r-1}f)(p^{r-1}x) = \phi(p^{r-1}h)(p^{r-1}x) = \overline{h(x)} = \overline{f(y)} = \phi(p^{r-1}f)(p^{r-1}y) =$
 $= \phi(p^{r-1}f)((g^{-1}x) = \phi(p^{r-1}f)(\gamma p^{r-1}x) = (\gamma \cdot \phi(p^{r-1}f))(p^{r-1}x)$. Donc ϕ est $\mathbb{K}[Y]$ -linéaire.

Comme la structure de $\mathbb{K}[Y]$ -module de $p^{r-1}M^*$ détermine entièrement M^* en vertu du théorème 4.17, il suffit de montrer que $p^{r-1}M^* \cong p^{r-1}M$, donc que $V \cong V^*$. On peut supposer que V est un $\mathbb{K}[Y]$ -module cyclique, donc de la forme $V = \mathbb{K}[Y]/(f)$. Si α est la matrice de Y dans une base de V , ${}^t\alpha$ est la matrice de Y dans la base duale. f est le polynôme minimal ainsi que le polynôme caractéristique de α . Comme l'un et l'autre sont conservés par transposition de α , ${}^t\alpha$ admet f à la fois comme polynôme minimal et comme polynôme caractéristique. C'est dire que $V^* \cong \mathbb{K}[Y]/(f)$. $\square$

Remarque : Dans le cas non modulaire, si G est abélien, alors tout AG -module A -libre M est isomorphe à son dual car M est déterminé par M/pM , et le résultat est clair sur un corps par la théorie des caractères (Rappelons encore qu'il ne s'agit pas de la définition classique de représentation duale). On peut donc légitimement se poser la question s'il ne s'agit pas là d'un résultat général pour les groupes abéliens, la difficulté étant bien sûr qu'il n'y a aucun espoir de trouver un isomorphisme canonique $M \rightarrow M^*$. Notons que la question n'a évidemment pas de sens pour un groupe non abélien car le dual d'un module à gauche est un module à droite.

Proposition 4.34 : Tout AC_p -module A -libre de type fini sans facteur projectif est isomorphe à son bicomplément.

Preuve : On a déjà vu que le passage au dual est un foncteur exact car A est un A -module injectif. Si $L \xrightarrow{f} M$ est une couverture projective de M et $N = \text{Ker} f$, alors $N \xrightarrow{g} L$ est une enveloppe injective de N car M est sans facteur projectif, en vertu de la proposition 2.21. Il en résulte que $L \cong L^* \xrightarrow{g^*} N^* \cong N$ est une couverture projective de N .

$\text{Ker} g^* \cong M^* \cong M$ et donc M est le complément de N , qui était lui-même le complément de M . $\square$

Corollaire 4.35 : Soit M un AC_p -module A -libre de type fini sans facteur projectif.

a) M admet une résolution projective périodique de période 2.

b) $\text{Ext}_{AC_p}^n(M, \mathbb{Z})$ et $\text{Tor}_{AC_p}^{AC^p}(M, \mathbb{Z})$ sont périodiques de période 2.

Preuve : b) résulte de a) et a) est un cas particulier de la proposition 2.23.

§10 Modules cohomologiquement triviaux

Nous allons calculer la cohomologie du groupe cyclique C_p à coefficients dans un AC_p -module A-libre de type fini M. La cohomologie d'un groupe cyclique d'ordre n est bien connue : les multiplications par g-1 et par $\sum_{k=0}^{n-1} g^k$ sont des endomorphismes de M et on a :

$\hat{H}^{2i+1}(C_p, M) = \text{Ker}(\sum g^k) / \text{Im}(g-1)$ et $\hat{H}^{2i}(C_p, M) = \text{Ker}(g-1) / \text{Im}(\sum g^k)$ pour tout $i \in \mathbb{Z}$. Il s'agit bien sûr de la cohomologie de Tate, cf. [Se 1, chap. VIII, §1]. Rappelons qu'un G-module M est dit cohomologiquement trivial si pour tout sous-groupe H de G et tout entier n, $\hat{H}^n(H, M) = 0$. Lorsque $G = C_p$, il n'y a bien sûr que le sous-groupe $H = G$ à considérer.

Rappelons qu'un module relativement projectif est cohomologiquement trivial, donc en particulier un AC_p -module libre l'est.

Soient M de type 1, L sa couverture projective et N son complément. On a une suite exacte $0 \rightarrow N \rightarrow L \rightarrow M \rightarrow 0$. Compte tenu du fait que L est cohomologiquement trivial, la suite exacte longue de cohomologie associée à cette suite exacte nous livre des isomorphismes : $\hat{H}^i(C_p, N) \cong \hat{H}^{i-1}(C_p, M)$.

Il suffit donc de calculer la cohomologie de C_p à coefficients dans un module de type 1. Comme ce calcul se généralise sans difficultés à celui de la cohomologie de C_p à coefficients dans un module de type 1, c'est ce dernier que nous allons entreprendre.

Proposition 4.36 : On suppose $r \geq 2s$. Soit M un AC_p^s -module de type 1, p étant impair. Soit $\phi \in \text{End}(p^{r-s}M)$ l'endomorphisme caractéristique de M, défini par $\phi(p^{r-s}x) = (g-1)x$. Alors : $\hat{H}^{2i+1}(C_p^s, M) = \text{Coker } \phi$, $\hat{H}^{2i}(C_p^s, M) \cong \text{Ker } \phi$.

Preuve : Par définition de ϕ , on a $gx = x + \phi(p^{r-s}x)$. g agit donc trivialement sur p^sM , ainsi que sur $p^{r-s}M$ car $p^{r-s}M \subset p^sM$ vu que $r \geq 2s$.

Alors : $\sum_{k=0}^{p^s-1} g^k x = x + (x + \phi(p^{r-s}x)) + \dots + (x + (p^s-1)\phi(p^{r-s}x)) =$
 $= p^s x + \frac{p^s(p^s-1)}{2} \phi(p^{r-s}x) = p^s x$ car p est impair et $p^s \phi(p^{r-s}x) = 0$.

La multiplication par $\sum g^k$ est égale à la multiplication par p^s . Donc
 $\text{Ker} \sum g^k = p^{r-s}M$ et $\text{Im} \sum g^k = p^s M$.

Reste à calculer $\text{Ker}(g-1)$ et $\text{Im}(g-1)$.

Par définition de ϕ , $\text{Im}(g-1) = \text{Im} \phi$ et par conséquent

$$\hat{H}^{2i+1}(C_{p^s, M}) = p^{r-s}M / \text{Im} \phi = \text{Coker} \phi. \quad \text{Ker}(g-1) = \{x \in M \mid \phi(p^{r-s}x) = 0\} = \\ = \{x \in M \mid p^{r-s}x \in \text{Ker} \phi\}$$

La multiplication par p^{r-s} fournit un homomorphisme surjectif $\text{Ker}(g-1) \rightarrow \text{Ker} \phi$
dont le noyau est $p^s M$ car $p^s M \subset \text{Ker}(g-1)$. Finalement :

$$\text{Ker} \phi \cong \text{Ker}(g-1) / p^s M = \hat{H}^{2i}(C_{p^s, M}). \quad \square$$

Corollaire 4.37 : Dans les hypothèses de la proposition, les conditions
suivantes sont équivalentes :

(1) M est cohomologiquement trivial (2) ϕ est injectif (3) ϕ est surjectif.

Preuve : Comme $p^{r-s}M$ est artinien et noethérien, (2) et (3) sont équivalents.
De plus ϕ est un isomorphisme si et seulement si $\hat{H}^1(C_{p^s, M}) = 0 \quad \forall i \in \mathbb{Z}$, par
la proposition. Cette dernière condition équivaut à dire que M est cohomolo-
giquement trivial comme on peut le voir par calcul explicite de la cohomolo-
gie des sous-groupes de C_p ou en appliquant un théorème bien connu de
Rim qui dit qu'un G -module M est cohomologiquement trivial si et seulement
si $\hat{H}^i(G_p, M) = 0$ pour tout $i \in \mathbb{Z}$ et pour tout sous-groupe de Sylow G_p de G . $\square$

Le théorème de Rim cité affirme en fait beaucoup plus (cf. [Ri] ou [Se 1, chap.
IX, §5] : les conditions suivantes sont équivalentes pour un $\mathbb{Z}G$ -module M :

(1) M est cohomologiquement trivial (2) $\text{proj dim}_{\mathbb{Z}G} M < \infty$ (3) $\text{proj dim}_{\mathbb{Z}G} M \leq 1$.

Donc si l'endomorphisme caractéristique ϕ d'un module M de type 1 est un
isomorphisme, alors M admet une résolution projective de longueur 1 comme
 $\mathbb{Z}C_p$ -module (la résolution ne peut être de longueur 0 puisque M n'est pas
projectif). Si cette résolution est $0 \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$, alors M repré-
sente un élément du groupe des classes de projectifs $K_0(\mathbb{Z}C_p)$, à savoir
 $[M] = [P_0] - [P_1]$ ($[M]$ est indépendant du choix de P_0 et P_1 par le lemme de
Schanuel). On peut montrer que, dans le cas $s = 1$ en tout cas, M représente

en fait zéro dans le groupe des classes de projectifs réduit $\hat{K}_0(\mathbb{Z}_p)$, la preuve étant basée sur le fait que M est un $\mathbb{Z}_p$ -module nilpotent. En d'autres termes, si on choisit P_0 libre, alors P_1 est stablement libre.

Revenons au cas $G = C_p$ pour montrer que "presque tous" les modules M de type 1 indécomposables sont cohomologiquement triviaux. En vertu de la proposition 4.36, il suffit de considérer l'endomorphisme caractéristique de M . Si M est indécomposable, le $K[Y]$ -module $N = p^{r-1}M$ l'est aussi, donc de la forme $N = K[Y]/(f)$ où f est une puissance d'un polynôme irréductible. Comme le déterminant de l'endomorphisme ϕ (multiplication par Y) est égal, au signe près, au terme constant de f et que ce dernier n'est nul que si f est une puissance de Y , ϕ est inversible, c'est-à-dire M est cohomologiquement trivial, si et seulement si f n'est pas une puissance de Y . Si $f = Y^n$, $\text{Ker } \phi \cong \text{Coker } \phi \cong K$ et donc la cohomologie est constante, égale à K . Par la propriété de décalage déjà vue, donnant la cohomologie des modules de type $p-1$ en fonction de celle des modules de type 1, le même résultat est valable pour les modules de type $p-1$. On a vu en effet dans la classification des modules de type $p-1$ (§6) que si ϕ est l'endomorphisme caractéristique d'un module M de type 1, alors $-\phi$ est celui du complément N de M et bien sûr ϕ est un isomorphisme si et seulement si $-\phi$ l'est.

Exemple : On prend $A = \mathbb{Z}/p^r\mathbb{Z}$ et $f = Y^n + \sum_{i=0}^{n-1} a_i Y^i \in \mathbb{Z}/p\mathbb{Z}[Y]$

Soit M le module de type 1 correspondant à $N = \mathbb{Z}/p\mathbb{Z}[Y]/(f)$. On suppose $a_0 \neq 0$ afin que M soit cohomologiquement trivial. La présentation de M comme $\mathbb{A}_p$ -module (§6) nous donne aisément une présentation de M comme $\mathbb{Z}_p$ -module :

Si $\alpha_i \in \mathbb{Z}$ a pour image a_i dans $\mathbb{Z}/p\mathbb{Z}$, on a :

$$M = \langle x_0, \dots, x_{n-1} \mid p^r x_i = 0 \ (i = 0, \dots, n-1), \ x_i = p^{r-1} x_{i+1} \ (i = 0, \dots, n-2), \ (g-1)x_{n-1} = -\sum_{i=0}^{n-1} p^{r-1} \alpha_i x_i \rangle.$$

Si P_0 est le $\mathbb{Z}_p$ -module libre engendré par $x_0, \dots, x_{n-1}$ et si P_1 est le sous-module de P_0 engendré par les relations définissant M , alors P_1 est projectif par le théorème de Rim. Plus précisément, dire que a_0 est non nul revient à dire que $p \nmid a_0$. On a donc : P_1 est projectif si et seulement si $p \nmid a_0$.

Par la remarque faite plus haut, P_1 est même stablement libre. Remarquons finalement que bien que M ait une résolution projective de longueur 1 comme $\mathbb{Z}_p$ -module, M n'admet pas de résolution projective finie comme $(\mathbb{Z}/p^r\mathbb{Z})C_p$ -module en vertu du corollaire 4.35.

§11 Modules de type k par Ext.

La classification des modules de type k par leur endomorphisme caractéristique (théorème 4.17) s'interprète de manière naturelle en termes d'algèbre homologique. Soient $G = C_p^s$, Q un diviseur unitaire de degré k de $X^{p^s}-1$, $R = (X^{p^s}-1)/Q$. On suppose $r \geq 2 (s - v_p(k))$ et on pose $e = r - s + v_p(k)$. L'hypothèse sur r revient à $e \geq r-e$ ou encore $r \leq 2e$. On pourra ainsi faire usage du théorème 4.17. Soient L un AG-module libre de rang n et $M = L/Q$.

$M \cong (A[X]/(Q))^n$ joue le rôle d'un module de type k "universel" (de rang nk) : tout module E de type k et de rang nk a été construit dans le théorème 4.17 comme étant le module M sur lequel on définit une nouvelle structure de AG-module (à l'aide de l'endomorphisme caractéristique de E), coïncidant avec celle de M sur $p^{r-e}M$, donc a fortiori sur $M/p^e M \cong p^{r-e}M$ ainsi que sur $p^e M \subset p^{r-e}M$ ($e \geq r-e$). Ainsi E apparaît comme extension $0 \rightarrow p^e M \rightarrow E \rightarrow M/p^e M \rightarrow 0$ et son endomorphisme caractéristique est un endomorphisme de $p^e E = p^e M$. Posons $\bar{M} = M/p^e M$. On sait (cf. [HS, chap. III]) que $\text{Ext}_{AG}^1(\bar{M}, p^e M)$ classe les extensions de $p^e M$ par $\bar{M}$ à isomorphisme d'extensions près (mais pas à isomorphisme de modules près).

Calcul de $\text{Ext}_{AG}^1(\bar{M}, p^e M)$

Soit $N \cong L/RL = (A[X]/(R))^n$. Soient $\pi: L \rightarrow M$ et $\rho: L \rightarrow N$ les projections canoniques. N est le complément de M et réciproquement. Soit en effet $\beta: M \rightarrow L$ et $\gamma: N \rightarrow L$ définis par $\beta(y) = Rx$ où x est tel que $\pi(x) = y$, et $\gamma(z) = Qx$ où x est tel que $\rho(x) = z$. β et γ sont bien définis car $\text{Ker } \pi$ est annulé par R et $\text{Ker } \rho$ par Q. On a alors deux suites exactes $0 \rightarrow M \xrightarrow{\beta} L \xrightarrow{\rho} N \rightarrow 0$, et $0 \rightarrow N \xrightarrow{\gamma} L \xrightarrow{\pi} M \rightarrow 0$. Notons j l'inclusion $p^e M \rightarrow M$ et q la projection $M \rightarrow \bar{M}$.

On considère le diagramme exact :

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \rightarrow & p^e N & \rightarrow & N & \xrightarrow{t} & N \rightarrow 0 \\
 & & \downarrow & & \downarrow \gamma & & \downarrow \\
 0 & \rightarrow & p^e L & \rightarrow & L & \rightarrow & \bar{L} \rightarrow 0 \\
 & & \downarrow & & \downarrow \pi & & \downarrow \\
 0 & \rightarrow & p^e M & \xrightarrow{j} & M & \xrightarrow{q} & \bar{M} \rightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

On associe à ce diagramme un diagramme de suites exactes longues d'Ext dans la première variable (contravariantes) :

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{Hom}_{\text{AG}}(\bar{L}, p^e M) & \longrightarrow & \text{Hom}_{\text{AG}}(L, p^e M) & & \\
 & & \downarrow & & \downarrow \gamma^* & & \\
 0 & \longrightarrow & \text{Hom}_{\text{AG}}(\bar{N}, p^e M) & \xrightarrow{t^*} & \text{Hom}_{\text{AG}}(N, p^e M) & \xrightarrow{\chi^*} & \text{Hom}_{\text{AG}}(p^e N, p^e M) \\
 & & \downarrow & & \downarrow \partial & & \downarrow \\
 \text{Hom}_{\text{AG}}(M, p^e M) & \xrightarrow{\star} & \text{Hom}_{\text{AG}}(p^e M, p^e M) & \xrightarrow{\delta} & \text{Ext}_{\text{AG}}^1(\bar{M}, p^e M) & \xrightarrow{q^*} & \text{Ext}_{\text{AG}}^1(M, p^e M) \xrightarrow{j^*} \text{Ext}_{\text{AG}}^1(p^e M, p^e M) \\
 & & & & \downarrow & & \\
 & & & & \text{Ext}_{\text{AG}}^1(L, p^e M) & &
 \end{array}$$

Les deux homomorphismes χ^* sont nuls car $\text{Hom}(X, p^e M) \rightarrow \text{Hom}(p^e X, p^e M)$ est nul pour tout AG-module X . En effet, si on a $f : X \rightarrow p^e M$, alors $\text{Ker } f \supset p^{r-e} X$ car p^{r-e} annule $p^e M$, et de plus $p^{r-e} X \supset p^e X$ car $e \geq r-e$. Par ailleurs, γ^* est nul car si on a $f : L \rightarrow p^e M$, alors $\text{Ker } f \supset QL$ car Q annule $p^e M$, et $QL = \text{Im } Y$. Donc $\gamma^*(f) = fY = 0$.

$\text{Ext}_{\text{AG}}^1(L, p^e M)$ est nul car L est libre. Ainsi ∂ est un isomorphisme. On en déduit aussitôt que $j^* = 0$ car $\star = 0$.

Le diagramme se réduit alors au suivant :

$$\begin{array}{ccccccc}
 & & \text{Hom}_{\text{AG}}(\bar{N}, p^e M) & \xrightarrow{t^*} & \text{Hom}_{\text{AG}}(N, p^e M) & & \\
 & & \downarrow \partial^* & & \downarrow \partial & & \\
 0 & \longrightarrow & \text{Hom}_{\text{AG}}(p^e M, p^e M) & \xrightarrow{\delta} & \text{Ext}_{\text{AG}}^1(\bar{M}, p^e M) & \xrightarrow{q^*} & \text{Ext}_{\text{AG}}^1(M, p^e M) \longrightarrow 0
 \end{array}$$

Il en résulte que q^* admet $\bar{\partial}(t^*)^{-1} \partial^{-1}$ comme section et qu'on a donc un isomorphisme : $\delta \oplus \bar{\partial}(t^*)^{-1} : \text{Hom}_{\text{AG}}(p^e M, p^e M) \oplus \text{Hom}_{\text{AG}}(N, p^e M) \xrightarrow{\sim} \text{Ext}_{\text{AG}}^1(\bar{M}, p^e M)$

Poursuivons le calcul en déterminant $\text{Hom}_{\text{AG}}(N, p^e M)$:

Posons $\bar{M} = M/p^{r-e}M$ et $\bar{N} = N/p^{r-e}N$. Comme $e \geq r-e$, ce sont des quotients de $\bar{M}$ et de $\bar{N}$ respectivement.

Vu que p^{r-e} et Q annulent $p^e M$, la projection $N \rightarrow \bar{N}/Q\bar{N}$ induit un isomorphisme $\text{Hom}_{\text{AG}}(N/QN, p^e M) \xrightarrow{\sim} \text{Hom}_{\text{AG}}(\bar{N}, p^e M)$.

Maintenant ρ induit un isomorphisme $L/(RL + QL) \xrightarrow{\sim} N/QN$ et de même π induit un isomorphisme $L/(RL + QL) \xrightarrow{\sim} M/RM$.

De plus, l'isomorphisme de multiplication par $p^e : \bar{M} \rightarrow p^e M$ induit un isomorphisme $\bar{M}/R\bar{M} \rightarrow p^e M/R(p^e M)$.

Finalement $p^e \cdot \pi \cdot p^{-1}$ induit un isomorphisme $\bar{N}/Q\bar{N} \xrightarrow{\sim} p^e M/R(p^e M)$ et par conséquent $\text{Hom}_{AG}(N, p^e M) \xrightarrow{\sim} \text{Hom}_{AG}(\bar{N}/Q\bar{N}, p^e M) \xrightarrow{\sim} \text{Hom}_{AG}(p^e M/R(p^e M), p^e M)$.

Ce dernier groupe d'homomorphismes consiste en les endomorphismes ϕ de $p^e M$ tels que $R\phi = 0$. On reconnaît là la condition imposée sur les endomorphismes caractéristiques dans le théorème 4.17.

Le premier facteur de la décomposition de $\text{Ext}_{AG}^1(\bar{M}, p^e M)$ en somme directe admet aussi l'interprétation suivante :

Soit $C = A[X]/(Q)$. On a une projection $AG \rightarrow C$ et donc tout C -module est un AG -module par restriction. Comme M est C -libre, $\text{Ext}_C^1(M, p^e M) = 0$ et on a donc :

$$\begin{array}{ccc} \text{Hom}_C(p^e M, p^e M) & \xrightarrow{\sim} & \text{Ext}_C^1(\bar{M}, p^e M) \rightarrow 0 = \text{Ext}_C^1(M, p^e M) \\ \parallel & & \downarrow \text{res} \\ 0 \rightarrow \text{Hom}_{AG}(p^e M, p^e M) & \xrightarrow{\delta} & \text{Ext}_{AG}^1(\bar{M}, p^e M) \end{array}$$

Par conséquent $\text{Im } \delta = \text{Im res}$ et le premier facteur de $\text{Ext}_{AG}^1(\bar{M}, p^e M)$ correspond aux extensions qui sont des C -modules.

Soit $B = C/p^{r-e}C$. $p^e M$ est un B -module (libre de rang n). On a donc finalement : $\text{Ext}_{AG}^1(\bar{M}, p^e M) \xrightarrow{\sim} \text{Hom}_B(p^e M, p^e M) \oplus \text{Hom}_B(p^e M/R(p^e M), p^e M)$

Théorème 4.38 : Soit E un module de type k , de rang nk (sur A). E peut être vu comme extension $0 \rightarrow p^e M \rightarrow E \rightarrow \bar{M} \rightarrow 0$.

Soit $\phi : p^e M \rightarrow p^e M$ l'endomorphisme caractéristique de E qu'on considère comme homomorphisme $\phi : p^e M/R(p^e M) \rightarrow p^e M$ (car $R \cdot \phi = 0$). Soit α la classe de l'extension E dans $\text{Ext}_{AG}^1(\bar{M}, p^e M)$. Alors la deuxième composante de α (dans la décomposition de $\text{Ext}_{AG}^1(\bar{M}, p^e M)$ en somme directe) est égale à ϕ .

Preuve : Soit $\{x_1, \dots, x_n\}$ une base de L et posons $y_1 = \pi(x_1)$, $z_1 = \rho(x_1)$. Les y_1 forment une base de M comme C -module et les z_1 une base de N comme $A[X]/(R)$ -module. On notera $\bar{y}_1$ la classe de y_1 dans $\bar{M}$, $\bar{y}_1$ sa classe dans $\bar{M}$ et de même pour $\bar{z}_1$ et $\bar{z}_1$.

Par l'isomorphisme $\text{Hom}_{\text{AG}}(p^e M/R(p^e M), p^e M) \cong \text{Hom}_{\text{AG}}(N, p^e M)$, ϕ est envoyé sur $\Psi: N \rightarrow p^e M$ défini par $N \rightarrow \bar{N}/Q\bar{N} \xrightarrow{\bar{\rho}} \bar{L}/(R\bar{L}+Q\bar{L}) \xrightarrow{\bar{\pi}} \bar{M}/R\bar{M} \xrightarrow{\bar{\rho}} p^e M/R(p^e M) \xrightarrow{\phi} p^e M$
 $\Psi(z_1) = \phi p^e \pi \rho^{-1} \bar{z}_1 = \phi p^e \bar{x}_1 = \phi p^e \bar{y}_1 = \phi(p^e y_1)$. On a :

$$\begin{array}{ccc} & \text{Hom}_{\text{AG}}(N, p^e M) & \\ & \cong \downarrow & \\ \text{Ext}_{\text{AG}}^1(\bar{M}, p^e M) & \xrightarrow{q^*} & \text{Ext}_{\text{AG}}^1(M, p^e M) \end{array}$$

et il s'agit de montrer que $q^* \alpha = \partial \Psi$. Par définition de ∂ , on considère :

$$\begin{array}{ccccccc} 0 & \rightarrow & N & \xrightarrow{\gamma} & L & \xrightarrow{\pi} & M \rightarrow 0 \\ & & \Psi \downarrow & & \downarrow \eta & & \downarrow \theta \\ 0 & \rightarrow & p^e M & \xrightarrow{\beta} & L & \xrightarrow{\zeta} & K \rightarrow 0 \end{array}$$

où $K = \text{Coker } \beta$, η étend $\beta \Psi$ (injectivité de L) et θ est induite par η .

On a $\text{Ext}_{\text{AG}}^1(M, p^e M) \cong \text{Hom}_{\text{AG}}(M, K)/\zeta_*(\text{Hom}_{\text{AG}}(M, L))$ (car $\text{Ext}_{\text{AG}}^1(M, L) = 0$ vu que L est injectif) et la classe de θ dans $\text{Ext}_{\text{AG}}^1(M, p^e M)$ est égale à $\partial \Psi$.

Par ailleurs, la classe caractéristique $\alpha \in \text{Ext}_{\text{AG}}^1(\bar{M}, p^e M)$ de l'extension $0 \rightarrow p^e M \rightarrow E \rightarrow \bar{M} \rightarrow 0$ est l'image de $\text{id}: p^e M \rightarrow p^e M$ par le "connecting" homomorphisme $\text{Hom}_{\text{AG}}(p^e M, p^e M) \rightarrow \text{Ext}_{\text{AG}}^1(\bar{M}, p^e M)$ associé à la suite exacte de l'extension.

On a $\text{Ext}_{\text{AG}}^1(\bar{M}, p^e M) \cong \text{Hom}_{\text{AG}}(\bar{M}, K)/\zeta_*(\text{Hom}_{\text{AG}}(\bar{M}, L))$ et α est la classe d'un homomorphisme $\mu: \bar{M} \rightarrow K$ déterminé par le diagramme :

$$\begin{array}{ccccccc} 0 & \rightarrow & p^e M & \rightarrow & E & \rightarrow & \bar{M} \rightarrow 0 \\ & & \parallel & & \downarrow \lambda & & \downarrow \mu \\ 0 & \rightarrow & p^e M & \xrightarrow{\beta} & L & \xrightarrow{\zeta} & K \rightarrow 0 \end{array}$$

$q^* \alpha \in \text{Ext}_{\text{AG}}^1(M, p^e M)$ est alors représenté par $\mu q: M \rightarrow K$.

Pour montrer que $q^* \alpha = \partial \Psi$, il faut donc montrer que θ et μq représentent le même élément de $\text{Ext}_{\text{AG}}^1(M, p^e M)$, c'est-à-dire que $\mu q - \theta \in \zeta_*(\text{Hom}_{\text{AG}}(M, L))$. Il reste à calculer μq et θ .

$\Psi: N \rightarrow p^e M$ est défini par $\Psi(z_1) = \phi(p^e y_1)$. Posons $p^e y'_1 = \phi(p^e y_1)$ et soit $x'_1 \in L$ tel que $\pi(x'_1) = y'_1$.

Alors $\beta\psi: N \rightarrow L$ est défini par $\beta\psi z_i = \beta p^e y'_i = \beta \pi p^e x'_i = R p^e x'_i$ par définition de β . Comme R annule N , R annule $R p^e x'_i$. Or on vérifie aisément que dans AG , et a fortiori dans L , tout élément annulé par R est multiple de Q . Donc $R p^e x'_i = Q p^e x''_i$ pour un certain x''_i . Parmi les $\eta: L \rightarrow L$ étendant $\beta\psi: N \rightarrow L$, on choisit η défini par $\eta(x_i) = p^e x''_i$, et il faut vérifier que $N \xrightarrow{\gamma} L$ commute :

$$\begin{array}{ccc} N & \xrightarrow{\gamma} & L \\ \beta\psi \searrow & & \nearrow \eta \\ & L & \end{array}$$

$\eta\gamma(z_i) = \eta Q x_i$ par définition de γ . Donc $\eta\gamma(z_i) = Q p^e x''_i = \beta\psi z_i$. Alors $\theta: M \rightarrow K$ induit par η est défini par $\theta\pi = \zeta\eta$, donc $\theta(y_i) = \theta\pi x_i = \zeta\eta x_i = \zeta p^e x''_i$.

Calculons maintenant μq . Il s'agit d'abord d'étendre $\beta: p^e M \rightarrow L$ en $\lambda: E \rightarrow L$. Comme $E = M$ avec une nouvelle structure de AG -module, les y_i engendrent E mais sont soumis maintenant aux relations $Q y_i = \phi(p^e y_i)$ par définition de l'endomorphisme caractéristique de E .

On choisit λ de la manière suivante : $\lambda(y_i) = R x_i + p^e x''_i$. On a $\lambda(p^e y_i) = R p^e x_i$ car $p^{2e} = 0$ ($2e \geq r$). De plus $\lambda(Q y_i) = Q p^e x''_i = R p^e x'_i$ car $QR = 0$.

Ces deux relations montrent d'une part que $\lambda(Q y_i - \phi(p^e y_i)) = R p^e x'_i - \lambda(p^e y'_i) = R p^e x'_i - R p^e x'_i = 0$, et donc λ est bien défini, d'autre part que $\lambda(p^e y_i) = R p^e x_i = \beta(p^e y_i)$, et donc λ étend bien β .

Il en résulte que $\mu': \bar{M} \rightarrow K$ induit par λ est défini par $\mu'(\bar{y}_i) = \zeta(R x_i + p^e x''_i)$. Finalement $\mu q: M \rightarrow K$ est donné par $\mu q(y_i) = \zeta(R x_i + p^e x''_i)$.

On a ainsi $(\mu q - \theta)(y_i) = \zeta R x_i$ et on veut montrer que $\mu q - \theta$ se relève en un homomorphisme de M dans L . Or ceci est évident car $\beta: M \rightarrow L$ satisfait à la question : $\beta(y_i) = R x_i$ par définition et donc $\zeta\beta(y_i) = \zeta R x_i = (\mu q - \theta)(y_i)$. $\square$

Remarques : 1) $\alpha \in \text{Ext}_{AG}^1(\bar{M}, p^e M)$ s'écrit $\alpha = \alpha_1 + \alpha_2$, $\alpha_1 \in \text{Hom}_B(p^e M, p^e M)$, $\alpha_2 \in \text{Hom}_B(p^e M/R \cdot (p^e M), p^e M)$. Comme $q^* \alpha = q^* \alpha_2$, on aurait pu travailler avec α_2 au lieu de α . $q^* \alpha_2$ est représenté par $\mu' q: M \rightarrow K$ pour un certain $\mu': \bar{M} \rightarrow K$ représentant α_2 . En déterminant μ' de manière "naturelle", on aurait eu alors déjà l'égalité des homomorphismes $\mu' q = \theta$. Ceci explique pourquoi seules les classes de μq et de θ dans $\text{Ext}_{AG}^1(M, p^e M)$ sont égales, alors que, toute la construction étant "naturelle", on aurait pu s'attendre à une égalité $\mu q = \theta$.

2) La raison pour laquelle la première composante α_1 de α ne joue pas de rôle est la suivante : on a vu que $\text{Im } \delta = \text{Im } (\text{res. Ext}_C^1(\bar{M}, p^e M) \rightarrow \text{Ext}_{AG}^1(\bar{M}, p^e M))$. Or les extensions E qu'on considère sont des C -modules de rang n (égaux à M), sur lesquels on met une nouvelle structure de AG -module, à l'aide de l'endomorphisme caractéristique ϕ . La deuxième composante $\alpha_2 = \phi$ caractérise cette nouvelle structure, alors que $\alpha_1 \in \text{Im res}$ décrit la structure de C -module de E .

Dire que $E = M$ comme C -module revient donc à dire que la première composante α_1 est constante pour toutes les extensions E qu'on considère. Or comme la classe caractéristique β de M est l'image par δ de l'identité de $p^e M$, on a $\beta = (\text{id}, 0)$. Par conséquent $\alpha = (\text{id}, \phi)$.

3) Si on voit M comme extension $0 \rightarrow p^{r-e} M \rightarrow M \rightarrow \bar{M} \rightarrow 0$ et si on utilise cette fois Ext comme foncteur covariant dans la seconde variable, on montre en dualisant toute la preuve que $\text{Ext}_{AG}^1(\bar{M}, p^{r-e} M) \cong \text{Hom}_{AG}(\bar{M}, \bar{M}) \oplus \text{Hom}_{AG}(\bar{M}, \bar{M}(R))$ où $\bar{M}(R) = \{x \in \bar{M} \mid Rx = 0\}$. En voyant l'endomorphisme caractéristique ϕ d'une extension E comme endomorphisme de $\bar{M}$ ($\bar{M} \cong p^e M$), dont l'image est annihilée par R , on montre que la classe caractéristique de E dans $\text{Ext}_{AG}^1(\bar{M}, p^{r-e} M)$ est là aussi (id, ϕ) .

4) On sait que Ext^1 classe les extensions à isomorphisme d'extensions près et non pas à isomorphisme de modules près. Dans notre cas, si ϕ et ϕ' sont deux endomorphismes de $p^e M$ équivalents, dans le sens que les deux structures de $B[Y]$ -module du B -module libre $p^e M$ sont isomorphes, alors les extensions E et E' correspondant à (id, ϕ) et (id, ϕ') respectivement sont isomorphes comme modules en vertu du théorème 4.17. Elles ne sont pas isomorphes comme extension si $\phi \neq \phi'$.

§12 Groupes à p -Sylow cyclique.

La classification des AC_p -modules A -libres du §6 fournit un algorithme théorique pour la détermination des AG -modules A -libres indécomposables, lorsque G est un groupe fini avec p -sous-groupe de Sylow C_p cyclique d'ordre p . Rappelons qu'en vertu du théorème de Maschke, tout AG -module est projectif relativement au sous-groupe C_p . En d'autres termes, tout AG -module est facteur direct d'un induit $AG \otimes_{AC_p} M$. Connaissant la liste des AC_p -modules indécomposables M , on trouve la liste de tous les AG -modules indécomposables en cherchant les facteurs indécomposables de tous les induits $AG \otimes_{AC_p} M$. Certes cette méthode reste impraticable en général, mais il serait intéressant d'étudier déjà certaines classes particulières de tels groupes, par exemple le cas où C_p est normal dans G , ou bien le cas où C_p admet un complément normal dans G .

Lorsque G est abélien, la classification est aisée sans même considérer les modules induits. G est nécessairement un produit direct $G = C_p \times H$ où H est un groupe d'ordre premier à p . On a alors :

$AG = A[H \times C_p] = AH[C_p]$. Or en vertu de la proposition 3.10 et du théorème 3.11, AH se décompose en $AH = \prod_{i=1}^n D_i$ où les D_i sont des anneaux courts ayant même uniformisante que A . En d'autres termes les D_i sont des extensions non ramifiées de A . Ce sont donc aussi des p -anneaux courts non ramifiés. Alors

$AG \cong \prod_{i=1}^n D_i C_p$ et tout AG -module M se décompose de manière unique en somme directe de $D_i C_p$ -modules : $M = \bigoplus_{i=1}^n M_i$. Exiger que M soit A -libre revient à dire que $M(p) = p^{r_p} M$ en vertu de la proposition 1.1. Or cette dernière condition est héritée par les M_i et par conséquent les M_i sont D_i -libres. Comme les D_i sont des p -anneaux courts non ramifiés, les $D_i C_p$ -modules D_i -libres sont connus et la classification est donc complète.

Il est clair que si $G = C_p \times H$, avec H abélien d'ordre premier à p , la classification des AG -modules se réduit à celle des AC_p -modules par le même argument.

Exemple : $G = C_{pm} \cong C_p \times C_m$, $(p,m) = 1$. En vertu de l'exemple de la fin du chapitre 3, on a $AC_m \cong \prod_{i=1}^n A[X]/(f_i)$ où les f_i sont les facteurs irréductibles de $X^m - 1$ (relevés à partir d'une décomposition $X^m - 1 = \prod \bar{f}_i$ sur $K = A/pA$).

$D_i = A[X]/(f_i)$ est un AC_m -module, l'action d'un générateur h de C_m se faisant par multiplication par X . Si M est un $D_i C_p$ -module D_i -libre de rang k , on a une action d'un générateur g de C_p sur M ainsi qu'une action de h sur $M = D_i^k$. Ces deux actions commutent et on en déduit aussitôt une action de gh , qui est générateur de G , sur M considéré comme A -module.

Si par exemple A contient une racine primitive m -ème de l'unité ω , $f_i = X - \omega^i$, $D_i = A$, et si $x \in M$, $(gh)x = g(\omega^i x) = \omega^i gx$.

CHAPITRE 5 : GROUPES DE GROTHENDIECK

§1 Généralités.

Soient A un anneau commutatif avec unité et G un groupe fini. L'algèbre du groupe $\Lambda = AG$ est un anneau avec unité. Or pour tout anneau Λ avec unité, on peut définir le groupe de Grothendieck d'une catégorie de Λ -modules de type fini : Soit $\underline{C}$ une sous-catégorie de la catégorie $\underline{M}_\Lambda$ de tous les Λ -modules de type fini. Soit L le groupe abélien libre engendré par les classes d'isomorphisme d'objets de $\underline{C}$. A toute suite exacte $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ d'objets et morphismes de $\underline{C}$, on associe l'expression $[M] - [M'] - [M'']$ de L , $[M]$ désignant la classe d'isomorphisme de M . Soit L_0 le sous-groupe de L engendré par ces expressions $[M] - [M'] - [M'']$. On définit le groupe de Grothendieck $K(\underline{C})$ de $\underline{C}$ comme étant $K(\underline{C}) = L/L_0$.

Si maintenant $\Lambda = AG$, trois cas sont particulièrement dignes d'intérêt :

Si $\underline{C} = \underline{M}_{AG}$, on désignera $K(\underline{C})$ par $T_A(G)$.

Si $\underline{C}$ est la sous-catégorie pleine de $\underline{M}_{AG}$ dont les objets sont les AG -modules de type fini qui sont projectifs comme A -modules, on désignera $K(\underline{C})$ par $R_A(G)$.

Si $\underline{C}$ est la sous-catégorie pleine de $\underline{M}_{AG}$ dont les objets sont les AG -modules projectifs de type fini, on désignera $K(\underline{C})$ par $P_A(G)$. A noter que, comme toute suite exacte de AG -modules projectifs est scindée, les relations définissant L_0 sont équivalentes aux relations $[M' \oplus M''] - [M'] - [M'']$. On retrouve ainsi la définition usuelle du groupe des classes de AG -modules projectifs de type fini $K_0(AG)$.

On a des homomorphismes "évidents" $P_A(G) \rightarrow R_A(G)$ et $R_A(G) \rightarrow T_A(G)$, chacun étant défini par $[M] \mapsto [M]$. Si $A = K$ est un corps, tout K -module est projectif et donc $R_K(G) = T_K(G)$. Si $|G|$ est inversible dans A , tout AG -module A -projectif est AG -projectif en vertu du théorème de Maschke et donc $P_A(G) = R_A(G)$. En particulier $P_K(G) = R_K(G) = T_K(G)$ si K est un corps de caractéristique première à $|G|$.

Si maintenant A est artinien, alors AG l'est aussi, et il résulte aisément du théorème de Jordan-Hölder que $T_A(G)$ est abélien libre sur l'ensemble $\{[S_1], \dots, [S_n]\}$ des classes d'isomorphisme de AG -modules simples. De même, en vertu du théorème de Krull-Schmidt, $P_A(G)$ est abélien libre sur l'ensemble $\{[P_1], \dots, [P_n]\}$ des classes d'isomorphisme de AG -modules projectifs indécomposables. En particulier, $T_A(G)$ et $P_A(G)$ sont isomorphes par l'isomorphisme

qui applique $[S_1]$ sur la classe d'isomorphisme $[P_1]$ de la couverture projective P_1 de S_1 . Mais l'homomorphisme canonique $P_A(G) \rightarrow T_A(G)$ (homomorphisme de Cartan) n'est en général pas un isomorphisme.

Sans hypothèses restrictives sur A , on peut munir $R_A(G)$ d'une structure d'anneau commutatif induite par le produit tensoriel : en reprenant la définition $R_A(G) = L/L_0$ d'un groupe de Grothendieck, on voit tout d'abord que le produit $[M] \cdot [N] = [M \otimes_A N]$ définit une structure d'anneau sur L , d'élément unité la classe $[A]$ du AG-module A avec action triviale de G . Si $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ est une suite exacte de AG-modules A -projectifs et si N est un AG-module A -projectif, alors $0 \rightarrow M' \otimes_A N \rightarrow M \otimes_A N \rightarrow M'' \otimes_A N \rightarrow 0$ est encore exacte, et par conséquent L_0 est un idéal de L . La structure d'anneau de L passe donc au quotient sur $R_A(G)$.

Pour plus de détails sur toutes ces questions, consulter $[G_1]$ ainsi que $[Se 2, §14]$.

Nous allons étudier de plus près ces groupes dans le cas d'un anneau court.

Soit A un anneau court de longueur r et d'uniformisante τ et soit $K = A/\tau A$ son corps résiduel.

Proposition 5.1 : $T_A(G) \stackrel{\sim}{=} T_K(G) = R_K(G)$.

Preuve : $T_A(G)$ est abélien libre sur l'ensemble des classes de AG-modules simples. Par la proposition 2.1, les AG-modules simples s'identifient aux KG-modules simples, qui sont générateurs libres de $T_K(G)$. $\square$

A noter que l'homomorphisme $A \rightarrow K$ n'induit pas d'homomorphisme $T_A(G) \rightarrow T_K(G)$ au moyen de l'extension des scalaires car une suite exacte de A -modules ne reste pas toujours exacte après tensorisation par K et les relations définissant $T_A(G)$ ne sont donc pas préservées. Il est donc nécessaire de définir l'isomorphisme $T_A(G) \stackrel{\sim}{=} T_K(G)$ sur les générateurs. A noter aussi que la structure d'anneau de $R_K(G)$ induit une structure d'anneau sur $T_A(G)$, mais l'homomorphisme canonique $R_A(G) \rightarrow T_A(G)$ n'est pas un homomorphisme d'anneaux (par exemple $1 \mapsto r$).

Proposition 5.2 : $P_A(G) \stackrel{\sim}{=} P_K(G)$.

Preuve : $P_A(G)$ est abélien libre sur l'ensemble des classes de AG-modules projectifs indécomposables. Par le corollaire à la proposition 3.1, cet ensemble est en bijection par réduction modulo π avec l'ensemble des classes de KG-modules projectifs indécomposables, et ces derniers sont générateurs libres de $P_K(G)$. $\square$

On a vu qu'on a aussi $T_A(G) \stackrel{\sim}{=} P_A(G)$ et $T_K(G) \stackrel{\sim}{=} P_K(G)$, l'image d'un générateur $[S_i]$ étant $[P_i]$ (respectivement $[Q_i]$), où P_i (resp. Q_i) est la couverture projective de S_i comme AG-module (resp. comme KG-module).

Ces résultats ne sont rien d'autre, dans une nouvelle formulation, que ceux du chapitre 3, §1.

Le groupe $R_A(G)$ est généralement plus difficile à calculer mais c'est aussi le plus intéressant, car il est non seulement muni d'une structure d'anneau mais même d'une structure de λ -anneau (cf. §3). Rappelons tout d'abord que si $f: A \rightarrow B$ est un homomorphisme d'anneaux, l'extension des scalaires de A à B induit un homomorphisme d'anneaux $f_*: R_A(G) \rightarrow R_B(G)$. En effet, l'extension des scalaires d'un AG-module A -projectif est un BG-module B -projectif et une suite exacte de AG-modules A -projectifs reste exacte après tensorisation par B .

Dans le cas non modulaire, c'est-à-dire lorsque la caractéristique de K ne divise pas $|G|$, $|G|$ est inversible dans A et $R_A(G) = P_A(G)$, $R_K(G) = P_K(G)$. L'extension des scalaires de A à K induit un isomorphisme $R_A(G) \xrightarrow{\sim} R_K(G)$ en vertu de la proposition 5.2. Or l'anneau $R_K(G)$ est bien connu : c'est l'anneau des représentations de G sur K , engendré par les caractères des représentations irréductibles de G sur K .

§2 $R_A(C_p)$.

On se place maintenant dans le cas modulaire et on suppose comme au chapitre 4 que A est un p -anneau court non ramifié de longueur $r \geq 2$. Pour $G = C_p$, nous avons déterminé la liste des AG-modules A -libres de type fini indécomposables ce qui va nous permettre de calculer $R_A(C_p)$, compte tenu du fait que tout A -module projectif est libre. Il n'est plus nécessaire de distinguer

comme précédemment le cas $p = 2$ du cas où p est impair, à condition de considérer lorsque $p = 2$, les modules de type 1 et de type 2-1 au sens de la définition du chapitre 4, §7. Rappelons que ces deux types de modules ne coïncident que si $r = 2$. Tout AG-module A-libre M se décompose en $M = M_1 \oplus M_{p-1} \oplus M_p$ où M_k est de type k . Lorsque $p = 2$ et $r = 2$, on posera par convention $M_{2-1} = 0$.

On reprend les notations de la définition d'un groupe de Grothendieck : L est le groupe abélien libre sur les classes d'isomorphisme $[M]$ de AG-modules A-libres M , L_0 est le sous-groupe de L engendré par les $[M_2] - [M_1] - [M_3]$ où $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ est exacte.

Proposition 5.3 : Soit L_1 le sous-groupe de L_0 engendré par les expressions $[M_2] - [M_1] - [M_3]$ correspondant à une suite exacte $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ de l'un des trois types suivants :

- I. M_1, M_2 et M_3 sont de type 1.
- II. M_1 est de type 1, M_2 est libre et M_3 est de type $p-1$.
- III. La suite est scindée.

Alors $L_1 = L_0$. Par conséquent $R_A(G) = L/L_1$.

Preuve : Soit $0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$ une suite exacte de AG-modules A-libres et $x = [M] - [N] - [Q]$ l'élément de L_0 correspondant. Il faut montrer que $x \in L_1$. On peut supposer que N est un sous-module de M et qu'il est non nul et propre.

1. Le cas où M est libre.

Si M est libre, M est injectif par la proposition 2.13. Par conséquent, l'injection $N \hookrightarrow M$ se factorise par l'enveloppe injective I de N : $M = I \oplus M'$ et $N \subset I$. Si $N = N_1 \oplus N_{p-1} \oplus N_p$ est une décomposition de N en types, alors $I = I_1 \oplus I_{p-1} \oplus I_p$ où I_k est l'enveloppe injective de N_k ($k=1, p-1, p$). De plus $I_p = N_p$ car N_p est libre, donc injectif. La suite exacte $0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$ se décompose alors en somme directe des suites exactes : $0 \rightarrow N_1 \rightarrow I_1 \rightarrow I_1/N_1 \rightarrow 0$, $0 \rightarrow N_{p-1} \rightarrow I_{p-1} \rightarrow I_{p-1}/N_{p-1} \rightarrow 0$, $0 \rightarrow N_p \rightarrow N_p \rightarrow 0 \rightarrow 0$ et $0 \rightarrow 0 \rightarrow M' \rightarrow M' \rightarrow 0$.

On a $[N] \equiv [N_1] + [N_{p-1}] + [N_p] \pmod{L_1}$, car aux suites exactes scindées correspondent des éléments L_1 , et de même avec M et Q . Il suffit donc de montrer que chacune des 4 suites définissent un élément de L_1 . C'est clair pour les deux dernières car elles sont scindées.

Maintenant par la proposition 2.22, I_1 est la couverture projective de I_1/N_1 et donc N_1 est le complément de I_1/N_1 . Il résulte alors de la proposition 4.14 que I_1/N_1 est de type $p-1$, ce qui montre que la première suite est du type II.

La relation $[I_{p-1}] - [N_{p-1}] - [I_{p-1}/N_{p-1}]$ provenant de la deuxième suite exacte est égale à celle définie par la suite des duals

$0 \rightarrow (I_{p-1}/N_{p-1})^* \rightarrow I_{p-1}^* \rightarrow N_{p-1}^* \rightarrow 0$. En effet le dual d'un module est isomorphe à ce module en vertu de la proposition 4.33. Par le même argument que pour la première suite, I_{p-1}/N_{p-1} doit être de type 1 et par conséquent $0 \rightarrow I_{p-1}/N_{p-1} \rightarrow I_{p-1} \rightarrow N_{p-1} \rightarrow 0$ est une suite du type II, ce qui achève la preuve dans le cas où M est libre.

2. On peut supposer N irréductible.

L_0 est engendré par les expressions $[M] - [N] - [Q]$ correspondant à des suites exactes $0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$ avec N irréductible. En effet, par récurrence sur le rang de N (comme A -module), si N' est un sous-module propre non nul de N , on a :

$$\begin{array}{ccc}
 \begin{array}{c} 0 \\ \downarrow \\ N' \\ \downarrow \\ 0 \end{array} & = & \begin{array}{c} 0 \\ \downarrow \\ N' \\ \downarrow \\ 0 \end{array} \\
 0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0 & & \\
 \downarrow & & \downarrow \\
 0 \rightarrow N/N' \rightarrow M/N' \rightarrow M/N \rightarrow 0 & &
 \end{array}
 \quad
 \begin{array}{l}
 [M] - [N] - [Q] = a - b + c \text{ où} \\
 a = [M] - [N'] - [M/N'] \\
 b = [N] - [N'] - [N/N'] \\
 c = [M/N'] - [N/N'] - [M/N]
 \end{array}$$

L'assertion en découle en appliquant l'hypothèse d'induction à a , b et c .

Il suffit donc de montrer qu'un générateur de L_0 appartient à L_1 , ce qui revient à supposer N irréductible.

3. On peut supposer N de type 1.

Comme N est irréductible, il est de type 1 ou de type $p-1$ car un module de type p , c'est-à-dire libre, n'est jamais irréductible. AG admet en effet l'idéal d'augmentation comme sous-module A -libre propre. Si N est de type $p-1$, soient $I \rightarrow N$ et $P \rightarrow Q$ les couvertures projectives de N et Q respectivement et soit $F = I \oplus P$. On a alors :

$$\begin{array}{ccccccc}
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \rightarrow & N' & \rightarrow & M' & \rightarrow & Q' \rightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \rightarrow & I & \rightarrow & F & \rightarrow & P \rightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \rightarrow & N & \rightarrow & M & \rightarrow & Q \rightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

par le premier pas du lemme classique permettant de construire des résolutions projectives au-dessus d'une suite exacte courte (cf. [HS, chap. III, §5]).

Soient alors : $x = [M] - [N] - [Q]$, $x' = [M'] - [N'] - [Q']$, $a = [F] - [I] - [P]$, $b = [I] - [N'] - [N]$, $c = [F] - [M'] - [M]$, $d = [P] - [Q'] - [Q]$.

On a $x = -x' + a + b - c + d$ et comme $a, b, c, d \in L_1$ en vertu du point 1,

$x \in L_1 \iff x' \in L_1$. Comme I est la couverture projective de N , N' est le complément de N et donc N' est de type 1. Il suffit de montrer que $x \in L_1$ et on est ainsi ramené au cas où le noyau est de type 1.

On raisonne désormais par récurrence sur le rang de M , ce qui permet de se ramener encore au cas suivant :

4. M n'a pas de sous-module propre non nul M' , facteur direct dans M , tel que $M' \cap N = 0$.

Si un tel M' existe, on a :

$$\begin{array}{ccccccc}
 & & \downarrow & & \downarrow & & \\
 & & M' & \xrightarrow{\sim} & (N \oplus M')/N & & \\
 & & \downarrow & & \downarrow & & \\
 0 & \rightarrow & N & \xrightarrow{\pi} & M & \rightarrow & M/N \rightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \rightarrow & (N \oplus M')/M' & \rightarrow & M/M' & \rightarrow & M/(N \oplus M') \rightarrow 0 \\
 & & & & \downarrow & & \downarrow \\
 & & & & 0 & & 0
 \end{array}$$

Soient alors : $a = [M] - [M'] - [M/M']$, $b = [M/N] - [M'] - [M/(N \oplus M')]$.

$c = [M/M'] - [N] - [M/(N \oplus M')]$. $a \in L_1$ car la suite correspondante est scindée par hypothèse. $b, c \in L_1$ par hypothèse d'induction. Donc $x = a - b + c \in L_1$.

Soit maintenant $M = M_1 \oplus M_{p-1} \oplus M_p$ une décomposition de M en types.

5. $N \cap M_{p-1} = 0$.

On suppose d'abord p impair. Soit $P = M[(g-1)^2] = \text{Ker } (g-1)^2 \subset M$.

$P = P \cap M_1 \oplus P \cap M_{p-1} \oplus P \cap M_p$. Par le lemme 4.20 appliqué au module M_{p-1} et au sous-module pM_{p-1} , on a $p \cdot (P \cap M_{p-1}) = 0$, donc $P \cap M_{p-1} \subset p^{r-1}M_{p-1}$, et $pP \cap M_{p-1} = 0$. Comme N est de type 1, $(g-1)^2 N = 0$, donc $N \subset P$. Soit alors $z \in N \cap M_{p-1}$. Si $p^k z \neq 0$ et $p^{k+1} z = 0$, quitte à remplacer z par $p^k z$, on peut supposer $pz = 0$. Alors $z \in p^{r-1}N \subset pN \subset pP$, et donc $z \in pP \cap M_{p-1} = 0$.

Si $p = 2$, et $r = 2$, $M_{2-1} = 0$ par convention. Si $r \geq 3$, on considère de nouveau $P = M((g-1)^2)$. $P \cap M_{2-1} \subset 2^{r-2}M_{2-1}$. En effet, si $x \in M_{2-1}$, $(g+1)x = 2^{r-1}y \in 2^{r-1}M_{2-1}$ par définition du type 2-1. Donc $(g-1)x = -2x + 2^{r-1}y$ et $(g-1)^2 x = -2(g-1)x = 4x$. Si $x \in P$, $4x = 0$ et $x \in 2^{r-2}M_{2-1}$. Ainsi $4P \cap M_{2-1} = 0$. Comme avant $N \subset P$ et si $z \in N \cap M_{2-1}$, on peut supposer $2z = 0$. Alors $z \in 2^{r-1}N \subset 4N$, car $r \geq 3$, et finalement $z \in 4N \cap M_{2-1} = 0$.

En vertu du point 4, on peut supposer $M_{p-1} = 0$.

6. Conclusion.

Si $N \cap M_p = 0$, on peut supposer, toujours par le point 4, que $M_p = 0$ et donc $M = M_1$. Dans ce cas $0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$ est une suite de modules de type 1, donc une suite de type I, et $x = [M] - [N] - [Q] \in L_1$. Si $N \cap M_p \neq 0$, on va montrer que $N \cap M_1 = 0$. On peut alors supposer $M_1 = 0$, donc $M = M_p$ et ce cas se résout par le point 1. Reste donc à montrer que si N est irréductible de type 1 et si $N \cap M_p \neq 0$, alors $N \cap M_1 = 0$.

Soit $0 \neq y \in N \cap M_p$. On peut supposer $py = 0$, donc $y = p^{r-1}x_0$, où $x_0 \in N$. Comme N est irréductible de type 1, $p^{r-1}N$ est un $K[Y]$ -module simple. Y agissant par l'endomorphisme caractéristique de N , et par conséquent $p^{r-1}x_0$ engendre $p^{r-1}N$ comme $K[Y]$ -module. Si $p^{r-1}N$ est de dimension n sur K , on pose $p^{r-1}x_1 = Y^i p^{r-1}x_0$ ($i = 0, \dots, n-1$). Les $p^{r-1}x_i$ forment une K -base de $p^{r-1}N$ et en conséquence $\{x_0, \dots, x_{n-1}\}$ est une A -base de N .

Montrons que $p^{r-1}N \subset M_p$ en montrant par récurrence sur i que $p^{r-1}x_i \in M_p$. $p^{r-1}x_0 \in M_p$ par construction de x_0 . Si $p^{r-1}x_1 \in M_p$, on a $x_1 \in M_p + pM$. Comme $pM = pM_1 \oplus pM_p$ et que $(g-1)pM_1 = 0$ car M_1 est de type 1, $(g-1) \cdot pM \subset pM_p$ et donc $(g-1)x_1 \in M_p$. Or par définition de l'endomorphisme caractéristique Y de N , $p^{r-1}x_{i+1} = Y p^{r-1}x_i = (g-1)x_i$ et donc $p^{r-1}x_{i+1} \in M_p$.

Soit alors $z \in N \cap M_1$. On peut supposer $pz = 0$, donc $z \in p^{r-1}N \subset M_p$. Alors $z \in M_1 \cap M_p = 0$ et il s'ensuit que $N \cap M_1 = 0$. $\square$

Les relations de L_1 du type II nous permettront d'écrire dans $R_A(G)$ un module de type $p-1$ comme différence d'un module libre et d'un module de type 1 (son complément). Quant aux relations du type I, elles nous ramènent à considérer des suites exactes, dans la catégorie des modules de type 1. Rappelons que tout sous-module A-libre d'un module de type 1 est de type 1 (lemme 4.24) et que bien sûr tout quotient d'un module de type 1 par un sous-module A-libre est encore de type 1. On définit une suite de composition d'un module M de type 1 comme étant une suite de sous-modules A-libres $M = M_0 \supset M_1 \supset \dots \supset M_{n-1} \supset M_n = 0$ telle que tous les quotients M_i/M_{i+1} soient irréductibles ($i = 0, \dots, n-1$).

Proposition 5.4 : Le théorème de Jordan-Hölder est vrai dans la catégorie des modules de type 1.

Preuve : On a vu au chapitre 4, §3 que $M \mapsto p^{r-1}M$ définit un foncteur exact de la catégorie des modules de type 1 dans la catégorie des $K[Y]$ -modules de dimension finie sur K et que ce foncteur envoie un module irréductible sur un $K[Y]$ -module simple. Par conséquent deux suites de composition de M fournissent deux suites de composition au sens usuel de $p^{r-1}M$ comme $K[Y]$ -module.

Par le théorème de Jordan-Hölder pour les $K[Y]$ -modules de longueur finie (i.e. de dimension finie sur K), ces deux suites ont même longueur et leurs quotients sont 2 à 2 isomorphes à l'ordre près. Or si P et Q sont deux modules de type 1, on a par le théorème 4.17 :
 $P \simeq Q \iff p^{r-1}P \simeq p^{r-1}Q$ (comme $K[Y]$ -modules). Il s'ensuit que les quotients irréductibles des deux suites de composition de M sont 2 à 2 isomorphes à l'ordre près. $\square$

Corollaire : Le groupe de Grothendieck de la catégorie des modules de type 1 est abélien libre sur les classes d'isomorphisme de modules de type 1 irréductibles. $\square$

Théorème 5.5 : Si p est impair ou si $r \geq 3$, $R_A(C_p)$ est abélien libre sur l'ensemble formé des classes d'isomorphisme de modules de type 1 irréductibles et de la classe du AC_p -module libre de rang 1. En d'autres termes :

$R_A(C_p) = R \oplus \mathbb{Z}$ où R est le groupe de Grothendieck de la catégorie des modules de type 1 et où le facteur $\mathbb{Z}$ est engendré par la classe du module libre de rang 1.

Preuve : Soit $F = A\mathbb{C}_p$ le module libre de rang 1 et soit $B = R \oplus \mathbb{Z}$. B est abélien libre sur $[F]$ ainsi que sur les irréductibles de type 1. On a un homomorphisme canonique $k : B \rightarrow R_A(\mathbb{C}_p)$ qui associe à un générateur de B sa classe dans $R_A(\mathbb{C}_p)$. Dans les notations de la proposition 5.3, on a $R_A(\mathbb{C}_p) = L/L_1$ et afin de construire une inverse à k , on va définir $h : L \rightarrow B$ nulle sur L_1 . Soit M un $A\mathbb{C}_p$ -module A -libre et $M = M_1 \oplus M_{p-1} \oplus M_p$ une décomposition de M en types. $M_p \cong F^m$ pour un certain m . Soit $F \xrightarrow{f} M_{p-1}$ la couverture projective de M_{p-1} et $N = \text{Ker } f$. Remarquons que dans $R_A(\mathbb{C}_p)$ on a $[M] = [M_1] - [N] + (n+m)[F]$. N est de type 1 car c'est le complément de M_{p-1} . Soient $S_1, \dots, S_s$ les facteurs de compositions de M_1 et $T_1, \dots, T_t$ ceux de N . Les S_i , les T_j ainsi que les entiers n et m sont univoquement déterminés par M (à isomorphisme près).

On pose alors $h([M]) = \sum_{i=1}^s [S_i] - \sum_{j=1}^t [T_j] + (n+m)[F]$. En reprenant la définition de L_1 dans la proposition 5.3, on voit que h est nul sur les relations du type I car si $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ est une suite exacte de modules de type 1, les facteurs de composition de M_2 sont la réunion de ceux de M_1 et de ceux de M_3 . h est nul sur les relations du type II car par construction même, on a remplacé tout module de type $p-1$ par la différence de sa couverture projective et de son complément (de type 1). C'est là qu'il faut supposer p impair ou $r \geq 3$ car si $p = 2$ et $r = 2$ les modules de type $2-1$ et de type 1 coïncident et les éléments de L_1 du type II sont des relations entre modules de type 1 et modules libres qui ne peuvent être nulles dans B . Enfin h est nul sur les relations du type III comme on le voit aisément en tenant compte, pour les facteurs de type $p-1$, du fait que la couverture projective d'une somme directe est la somme directe des couvertures projectives et que le complément d'une somme directe est la somme directe des compléments.

Ceci démontre que h induit $h : R_A(\mathbb{C}_p) \rightarrow B$ et on a trivialement $h \circ k = \text{id}$. Le fait que $k \circ h = \text{id}$ résulte du fait que dans $R_A(\mathbb{C}_p)$, on a, dans les notations ci-dessus, $[M] = \sum_{i=1}^s [S_i] - \sum_{j=1}^t [T_j] + (n+m)[F]$, comme on l'a remarqué en cours de démonstration. $\square$

Comme indiqué en cours de démonstration, la situation est différente dans le cas $p = 2$ et $r = 2$ car il y a des relations entre modules de type 1 et modules libres. Plus précisément, le complément N d'un module M de type 1 est encore de type 1 et $[N] + [M]$ doit être identifié à la couverture projective de M en vertu des relations du type II.

Si M est un module de type 1 irréductible, alors $2M$ est un $K[Y]$ -module simple, donc isomorphe à $K[Y]/(f)$ où f est un polynôme irréductible sur K . Si E est l'ensemble des polynômes unitaires irréductibles sur K , on a une correspondance bijective entre les classes d'isomorphisme de modules irréductibles de type 1 et les éléments de E . On désignera par M_f le module correspondant à $f \in E$. Si $d^\circ f$ désigne le degré de f , $d^\circ f$ est aussi le rang de M_f , car c'est la dimension de $2M_f \cong K[Y]/(f)$.

Par la proposition 4.28, si ϕ est l'endomorphisme caractéristique de M , $\phi + id$ est l'endomorphisme caractéristique du complément N et M . Si $M = M_f$, f est le polynôme caractéristique de ϕ et par conséquent $\bar{f}(Y) = f(Y+1)$ est le polynôme caractéristique de $\bar{\phi} = \phi + id$. C'est aussi son polynôme minimal car f est irréductible et donc $2N \cong K[Y]/(\bar{f})$. Ainsi $N \cong M_{\bar{f}}$.

Ceci démontre que le passage au complément d'un module irréductible de type 1 correspond à l'involution de E envoyant f sur $\bar{f}$ où $\bar{f}(Y) = f(Y+1)$.

Soient E_0 l'ensemble des points fixes de E par cette involution, E_1 un système de représentants des orbites à 2 éléments de l'involution et $\bar{E}_1$ l'ensemble des $\bar{f} \in E$ où f parcourt E_1 . On a $E_0 \cup E_1 \cup \bar{E}_1$. Il n'y a semble-t-il pas de manière canonique de choisir des représentants des orbites pour construire E_1 .

Les polynômes g de E_0 correspondent aux modules M_g isomorphes à leur complément.

Désignons comme auparavant par F le module libre de rang 1.

Théorème 5.6 : Soit A un 2-anneau court non ramifié de longueur 2.

$$R_A(C_2) = \langle [M_g], g \in E_0; [M_f], f \in E_1; [F] \mid 2[M_g] = d^\circ g [F], g \in E_0 \rangle$$

Preuve : Soit $B = \langle [M_g], g \in E_0; [M_f], f \in E_1; [F] \mid 2[M_g] = d^\circ g [F], g \in E_0 \rangle$

On a un homomorphisme canonique $k : B \rightarrow R_A(C_2)$ qui envoie un générateur de B sur sa classe dans $R_A(C_2)$. k est bien défini car les relations définissant B sont envoyées sur les relations de $R_A(C_2)$ correspondant aux suites exactes $0 \rightarrow M_g \rightarrow F^{d^0 g} \rightarrow M_g \rightarrow 0$. Il s'agit bien d'une suite exacte, car comme M_g est de type 1 et de rang $d^0 g$ sur A , sa couverture projective est libre de rang $d^0 g$, et le noyau est le complément de M_g , qui est isomorphe à M_g car $g \in E_0$. Par la proposition 5.3, on a $R_A(C_2) = L/L_1$ et on va définir $h: L \rightarrow B$, nulle sur L_1 . Soit M un AC_2 -module A -libre et $M = M_1 \oplus M_2$ une décomposition de M en types. $M_2 \cong F^m$ pour un certain m . Soient $S_1, \dots, S_n$ les facteurs de composition de M_1 . Comme S_i est irréductible, $S_i \cong \mathbb{A}_{f_i}$, $f_i \in E$.

Si $U = \{f_1, \dots, f_n\}$, notons $U_0 = \{f \in U \mid f \in E_0\}$, $U_1 = \{f \in U \mid f \in E_1\}$ et $U_2 = \{f \in U \mid f \in E_2\}$. $U = U_0 \cup U_1 \cup U_2$. Pour $f \in U_2$, on a une suite exacte $0 \rightarrow M_{\bar{f}} \rightarrow F^{d^0 f} \rightarrow M_f \rightarrow 0$ car $F^{d^0 f}$ est la couverture de M_f et $M_{\bar{f}}$ son complément.

Remarquons que dans $R_A(C_2)$, on a : $[M] = \sum_{i=1}^n [S_i] + m[F]$, donc $[M] = \sum_{g \in U_0} [M_g] + \sum_{f \in U_1} [M_f] + \sum_{f \in U_2} (d^0 f [F] - [M_{\bar{f}}]) + m[F]$.

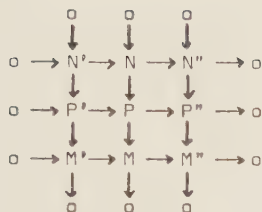
Comme $\bar{f} \in E_1$ si $f \in U_2$, $[M_{\bar{f}}]$ est un générateur de B et on peut poser : $h[M] = \sum_{g \in U_0} [M_g] + \sum_{f \in U_1} [M_f] - \sum_{f \in U_2} [M_{\bar{f}}] + (m + \sum_{f \in U_2} d^0 f [F])$.

Comme dans le théorème précédent, on vérifie aisément que h est nul sur les relations de L_1 des types I et III. Les relations du type II sont de la forme $0 \rightarrow N \rightarrow P \rightarrow M \rightarrow 0$ où M est de type 1, P sa couverture projective et N son complément. On montre que $h[P] - h[N] - h[M] = 0$ par récurrence sur le nombre k des facteurs de composition de M . Si $k = 1$, $M = \mathbb{A}_{\bar{f}}$, $f \in E$, $N = M_{\bar{f}}$, et $P = F^{d^0 f}$.

Si $f \in E_0$, $f = \bar{f}$ et $d^0 f [F] - [M_{\bar{f}}] - [M_{\bar{f}}]$ est une relation dans B par définition de B . Si $f \in E_2$, $h[M] = [P] - [N]$ par définition de h .

Si $f \in E_1$, on a aussi une suite exacte $0 \rightarrow \mathbb{A}_{\bar{f}} \rightarrow F^{d^0 f} \rightarrow M_{\bar{f}} \rightarrow 0$ car $F^{d^0 f}$ est aussi la couverture projective de $M_{\bar{f}}$ (c'est en fait la suite des duals) et comme $\bar{f} \in E_2$, on est ramené au cas précédent.

Si maintenant $k > 1$, soient M' un sous-module A -libre propre non nul de M et $M'' = M/M'$. Soient P' la couverture projective de M' et P'' celle de M'' . P' est libre de rang $rg_A(M')$ et P'' est libre de rang $rg_A(M'')$. Comme P est libre de rang $rg_A(M') + rg_A(M'')$, $P \cong P' \oplus P''$ et il en résulte un diagramme exact :



$h[N] = h[N'] + h[N'']$ et $h[M] = h[M'] + h[M'']$ car h est nul sur les relations de type I. $h[P] = h[P'] + h[P'']$ car la suite est scindée et h est nul sur les relations du type III. $h[P'] = h[N'] + h[M']$ et $h[P''] = h[N''] + h[M'']$ par hypothèse d'induction. Il en résulte que $h[P] = h[N] + h[M]$.

A remarquer que ce même argument d'induction montre que les facteurs de composition du complément N de M sont les compléments des facteurs de composition de M . Il reste alors à vérifier que h est l'inverse de k .

$h \circ k = \text{id}$ trivialement. $k \circ h = \text{id}$ car, comme on l'a remarqué, on a dans $R_A(C_2)$:

$$[M] = \sum_g e_{U_0} [M_g] + \sum_f e_{U_1} [M_f] - \sum_f e_{U_2} [M_f] + (m + \sum_f e_{U_2} d^{\bullet} f [F]). \quad \square$$

Remarque : Il peut arriver que $R_A(C_2)$ soit abélien libre. Si par exemple K est algébriquement clos, tout polynôme $f \in E$ est de degré 1 et par conséquent $\bar{f}(Y) = f(Y+1) = f(Y)+1$ et $f \neq \bar{f}$. Il s'ensuit que $E_0 = \emptyset$ et il n'y a plus de relations.

Si en revanche il y a beaucoup de polynômes $f \in E$ tels que $f = \bar{f}$, il peut y avoir de la 2-torsion dans $R_A(C_2)$. Par exemple $K = \mathbb{Z}/2\mathbb{Z}$, $f = Y^8 + Y^6 + Y^5 + Y^3 + 1$, $g = Y^8 + Y^6 + Y^5 + Y^4 + Y^3 + Y + 1$, f et g sont irréductibles et $f = \bar{f}$, $g = \bar{g}$.

Alors $2([M_f] - [M_g]) = d^{\bullet} f [F] - d^{\circ} g [F] = 0$ mais $[M_f] - [M_g] \neq 0$ car les relations ont toujours des coefficients pairs dans les $[M_f]$, $h \in E_0$. De même si $f = Y^2 + Y + 1$, $g = Y^4 + Y + 1$, $h = Y^6 + Y^5 + Y^3 + Y^2 + 1$, f , g et h sont irréductibles, $f = \bar{f}$, $g = \bar{g}$, $h = \bar{h}$. Alors $2([M_f] + [M_g] - [M_h]) = 0$.

Nous allons voir un critère pour qu'un polynôme f sur un corps fini soit irréductible et satisfasse $f = \bar{f}$.

Soient K un corps de caractéristique 2 et $f \in K[Y]$. $f = \bar{f}$ si et seulement si il existe $g \in K[X]$ tel que $f(Y) = g(Y^2+Y)$. En effet, si $f(Y) = g(Y^2+Y)$, $\bar{f}(Y) = g((Y+1)^2 + (Y+1)) = g(Y^2+Y) = f(Y)$. Réciproquement, si $f = \bar{f}$, on raisonne par récurrence sur le degré n de f , le cas $n = 0$ étant trivial. On a $f(0) = f(1)$ et par conséquent $f(Y) - f(0)$ s'annule en 0 et en 1. Donc $f(Y) - f(0) = (Y^2+Y)f_1(Y)$. Alors $f_1 = \bar{f}_1$ et f_1 est de degré $n-2$. $f_1(Y) = g_1(Y^2+Y)$ et il s'ensuit que $f(Y) = (Y^2+Y)g_1(Y^2+Y) + f(0) = g(Y^2+Y)$, où $g(X) = X g_1(X) + f(0)$.

On considère l'extension quadratique $K(X)[Y]/(Y^2+Y+X) \cong K(X)$ du corps $K(X)$. $K[Y]$ est entier sur $K[X]$ et comme $K[Y]$ est intégralement clos, car factoriel, c'est l'anneau des entiers sur $K[X]$ de l'extension. Comme Y et $Y+1$ sont les deux zéros du polynôme minimal Y^2+Y+X de Y sur $K(X)$, l'extension est galoisienne de groupe de Galois cyclique d'ordre 2 engendré par $\sigma : f(Y) \mapsto \bar{f}(Y) = f(Y+1)$. Le fait que $f = \bar{f}$ si et seulement si $f(Y) = g(Y^2+Y)$, pour un $g \in K[X]$, correspond au fait que $K(X) = K(Y^2+Y)$ est le corps fixe de σ . Si $f(Y) = g(Y^2+Y)$ est irréductible, alors $g(X) \in K[X]$ l'est aussi. Réciproquement, si $g(X)$ est irréductible, alors dire que $f(Y) = g(Y^2+Y)$ est irréductible revient à dire que g reste premier par l'extension quadratique. Si $g(X)$ est irréductible mais ne reste pas premier par l'extension, on a $g(Y^2+Y) = f(Y)\bar{f}(Y)$ avec f irréductible, $f \neq \bar{f}$ sinon $f(Y) = h(Y^2+Y)$ et $g(Y^2+Y) = h(Y^2+Y)^2$ contrairement au caractère irréductible de g . Ainsi aucun premier de $K[X]$ ne ramifie dans $K[Y]$, car $(f) \neq (\bar{f})$ si $f \neq \bar{f}$.

Finalement l'ensemble E_0 des polynômes irréductibles $f \in K[Y]$ tels que $f = \bar{f}$ est obtenu comme l'ensemble des polynômes irréductibles $g \in K[X]$ qui restent irréductibles dans l'extension quadratique, mais vus dans $K[Y]$, c'est-à-dire de la forme $f(Y) = g(Y^2+Y)$. Si $K = \mathbb{F}_2$ est le corps fini à 2 éléments, ces polynômes sont caractérisés par le critère suivant, dû à Agou :

Soit $g \in K[X]$ un polynôme irréductible de degré n . Alors : $f(Y) = g(Y^2+Y)$ est irréductible $\Leftrightarrow f(Y) \mid Y^{2^{sn}} + Y + 1 \Leftrightarrow g(X) \mid X^{2^{sn-1}} + X^{2^{sn-2}} + \dots + X^4 + X^2 + 1$. Un autre critère, dû aussi à Agou, est le suivant :

Si $g = X^n + aX^{n-1} + \dots$ est irréductible, alors :

$f(Y) = g(Y^2+Y)$ est irréductible $\Leftrightarrow \text{Tra} \neq 0$, où Tr désigne la trace de l'extension $\mathbb{F}_2/\mathbb{F}_2$. Cette condition est bien sûr encore équivalente à $\text{Tra} = 1$. Pour plus de détails, on consultera [Ag].

La recherche des facteurs irréductibles g de degré n du polynôme $\sum_{k=0}^{sn-1} X^{2^k} + 1$ fournit de nombreux exemples. Si $K = \mathbb{F}_2$ ($s = 1$), la liste des g pour les petites valeurs de n est la suivante :

n	1	2	3	4	etc
$g(X)$	$X+1$	X^2+X+1	X^3+X^2+1	$X^4+X^3+1, X^4+X^3+X^2+X+1$	
$f(Y)=g(Y^2+Y)$	Y^2+Y+1	Y^4+Y+1	$Y^6+Y^5+Y^3+Y^2+1$	$Y^8+Y^6+Y^5+Y^3+1, Y^8+Y^6+Y^5+Y^4+Y^3+Y+1$	

Le nombre de tels polynômes augmente beaucoup lorsque n croît : il y en a 3 pour $n = 5$, 5 pour $n = 6$, 9 pour $n = 7$, 16 pour $n = 8$, etc.

L'extension quadratique considérée permet de donner une autre description du groupe de Grothendieck : le sous-groupe engendré par $[F]$ est infini cyclique car si $n[F] = 0$, alors, dans le groupe libre sur les générateurs de $R_A(C_2)$, on aurait $n[F] = \sum_f \lambda_f (2[M_f] - d^0 f[F])$, ce qui n'est possible que si tous les λ_f sont nuls, et donc si $n = 0$. Soit $\tilde{R}_A(C_2) = R_A(C_2) / \langle [F] \rangle$. C'est en fait l'anneau quotient de $R_A(C_2)$ par l'idéal des projectifs. Le calcul de $R_A(C_2)$ nous livre alors : $\tilde{R}_A(C_2) = (\bigoplus_{f \in E_1} \mathbb{Z} \cdot [M_f]) \oplus (\bigoplus_{f \in E_0} \mathbb{Z}/2\mathbb{Z} \cdot [M_f])$.

Dans $\tilde{R}_A(C_2)$, on a $[M_f^-] = -[M_f]$ et en réintroduisant des générateurs $[M_f]$ pour $f \in \bar{E}_1$, on peut écrire : $\tilde{R}_A(C_2) = \langle [M_f], f \in E \mid [M_f] + [M_f^-] = 0 \rangle$.

Comme $K[Y]$ est factoriel, $K(Y)^* \cong K^* \times \prod_{f \in E} \mathbb{Z} \cdot f$. Donc en passant de la notation additive à la notation multiplicative, on a :

$$\langle [M_f], f \in E \rangle \cong K(Y)^*/K^*, [M_f] \text{ étant envoyé sur } f.$$

Par cet isomorphisme, l'élément $[M_f] + [M_f^-]$ correspond à la norme $N(f) = f\bar{f}$.

Or $\text{Im} N = \langle f\bar{f} \mid f \in E \rangle \times (K^*)^2$, si bien que :

$$K(Y)^*/\text{Im} N = \langle f \mid f \in E \rangle / \langle f\bar{f} \mid f \in E \rangle \times K^*/(K^*)^2 \cong \tilde{R}_A(C_2) \times K^*/(K^*)^2.$$

En particulier, si K est parfait, $\tilde{R}_A(C_2) \cong K(Y)^*/\text{Im} N$, et on vérifie aisément que le sous-groupe $\bigoplus_{f \in E} \mathbb{Z}/2\mathbb{Z} \cdot [M_f]$ s'identifie par cet isomorphisme au sous-groupe $K(X)^*/\text{Im} N$, qui n'est autre que le 2ème groupe de cohomologie galoisienne $H^2(C_2, K(Y)^*)$, C_2 étant le groupe de Galois de l'extension $K(Y)/K(X)$.

§3 Opérations d'Adams

On a vu que le produit tensoriel induit une structure d'anneau sur $R_A(G)$. Dans le cas où A est un p -anneau court non ramifié et où $G = C_p$, on dispose des résultats d'Hannula exposés au chapitre 4, §6, qui donnent la décomposition en indécomposables du produit tensoriel de deux modules indécomposables. La formule donnée dans le cas où les deux modules sont irréductibles de type 1 s'applique alors directement dans $R_A(C_p)$ et décrit entièrement la structure d'anneau de $R_A(C_p)$.

En outre, $R_A(G)$ est muni d'une structure de λ -anneau, c'est-à-dire, sans entrer dans les détails de la définition, que les puissances extérieures induisent des opérations $\lambda^i : R_A(G) \rightarrow R_A(G)$, définies par $\lambda^i[M] = [\Lambda^i M]$ où $\Lambda^i M$ est la i -ème puissance extérieure de M comme A -module, munie de l'action diagonale de G . On convient que $\lambda^0 x = 1$ pour tout $x \in R_A(G)$ et on a $\lambda^1 = \text{id}$.

On considère l'anneau $R_A(G)[[t]]$ des séries formelles en t à coefficients dans $R_A(G)$ et on définit $\lambda_t : R_A(G) \rightarrow R_A(G)[[t]]$ par $\lambda_t(x) = \sum_{i=0}^{\infty} \lambda^i(x) t^i$.

$\lambda_t(x)$ est inversible pour tout x car son terme constant est $\lambda^0(x) = 1$. On peut démontrer la formule $\lambda^k(x+y) = \sum_{i=0}^k \lambda^i(x) \cdot \lambda^{k-i}(y)$, qui est bien connue dans le cas d'une somme directe de modules. Il en résulte que λ_t est un homomorphisme du groupe additif de $R_A(G)$ dans le groupe multiplicatif des unités de $R_A(G)[[t]]$.

On définit alors $\Psi_t : R_A(G) \rightarrow R_A(G)[[t]]$ par $\Psi_t(x) = -t \lambda_t(x)^{-1} \frac{d}{dt} \lambda_t(x)$ ainsi que $\Psi_k : R_A(G) \rightarrow R_A(G)$ par la formule $\Psi_t(x) = \sum_{k=1}^{\infty} (-1)^k \Psi_k(x) t^k$.

Comme la dérivée logarithmique $dx = x^{-1} \frac{d}{dt} x$ satisfait $d(xy) = dx + dy$, on voit que Ψ_t , et a fortiori chaque Ψ_k , est un homomorphisme additif. Les Ψ_k sont appelés les opérations d'Adams de $R_A(G)$. En égalant les coefficients de $\lambda_t(x) \cdot \Psi_t(x)$ et de $-t \frac{d}{dt} \lambda_t(x)$, on voit que les Ψ_k peuvent être définis par récurrence à l'aide des formules :

$$\Psi_k = \Psi_{k-1} \cdot \lambda^1 + \Psi_{k-2} \cdot \lambda^2 - \dots + (-1)^{k-1} \Psi_1 \cdot \lambda^{k-1} + (-1)^k k \lambda^k = 0, \text{ où } \Psi_i \cdot \lambda^j(x) = \Psi_i(x) \cdot \lambda^j(x)$$

Il résulte aisément des définitions que $\Psi_1 = \text{id}$, que Ψ_k préserve le rang (sur A) des AG -modules, que si M est de rang 1, alors $\Psi_k[M] = [M]^k$, et enfin que Ψ_k commute aux homomorphismes de restriction de groupes $\rho^* : R_A(G) \rightarrow R_A(G')$ pour (pour $\rho : G' \rightarrow G$) ainsi qu'aux homomorphismes d'extension des scalaires

$f_* : R_A(G) \rightarrow R_{A'}(G)$ (pour $f : A \rightarrow A'$). De plus, à l'aide d'un "splitting principle" qui réduit le problème au cas trivial des modules de rang 1, Swan démontre, utilisant des techniques de géométrie algébrique, que les Ψ_K sont des endomorphismes de λ -anneau, i.e. $\Psi_K(xy) = \Psi_K(x)\Psi_K(y)$ et $\Psi_K\lambda^1 = \lambda^1\Psi_K$, et qu'ils satisfont en outre les relations $\Psi_K\Psi_1 = \Psi_1\Psi_K = \Psi_{K1}$ (cf. [Sw]). Kratzer a redémontré récemment ce résultat par des méthodes purement algébriques. Pour plus de détails sur les opérations d'Adams on peut consulter sa thèse [Kr], ainsi que [Ke] dans le cas où A est un corps.

Comme amuse-gueule final, nous allons calculer les opérations d'Adams sur $R_A(G)$ dans les cas que nous avons considérés jusqu'ici.

Cas non modulaire

Soient A un anneau court de corps résiduel K et G un groupe fini d'ordre premier à la caractéristique de K . On a vu que l'extension des scalaires de A à K induit un isomorphisme $R_A(G) \xrightarrow{\sim} R_K(G)$. Comme les Ψ_K commutent aux homomorphismes d'extension des scalaires, on est réduit à calculer les opérations d'Adams sur $R_K(G)$. Mais pour un corps, le résultat est bien connu (cf. [Ke]) : Si M est un KG -module de type fini, et si χ est le caractère de la représentation définie par M , alors $\Psi_K[M] = [\Psi_K M]$ où $\Psi_K M$ est le KG -module défini par le caractère $\Psi_K \chi$ suivant : $(\Psi_K \chi)(g) = \chi(g^K)$, $g \in G$.

En particulier, si G est abélien, alors, quitte à étendre les scalaires, on peut supposer que K est un corps de décomposition du groupe G . Ce n'est pas une hypothèse restrictive car si L est une extension de K , l'homomorphisme $R_K(G) \rightarrow R_L(G)$ est injectif. Mais alors tout KG -module simple est de dimension 1 sur K et si χ est le caractère correspondant au module simple S , alors la formule $(\Psi_K \chi)(g) = \chi(g^K)$ s'interprète en termes de module de la manière suivante : $\Psi_K S = S$ comme K -espace vectoriel (dimension 1) et $g \in G$ agit sur $\Psi_K S$ comme g^K agissait sur S . En d'autres termes, $\Psi_K S = \rho_K^* S$ où $\rho_K^* : R_K(G) \rightarrow R_K(G)$ est l'homomorphisme de restriction de groupes induit par l'homomorphisme de groupes $\rho_K : G \rightarrow G$ défini par $\rho_K(g) = g^K$.

Cas modulaire, $G = C_p$

Soit A un p -anneau court non ramifié de longueur r et de corps résiduel K . On se bornera au cas où soit p est impair, soit r est supérieur ou égal à 3. Dans ce cas, $R_A(C_p)$ est abélien libre sur le libre de rang 1 et sur les modules irréductibles de type 1. On pose comme avant $F = AC_p$ et nous allons tout d'abord calculer $\Psi_k[F]$.

Lemme 5.7 : $\Lambda^k F \cong F^{\binom{p}{k}}$ si $0 < k < p$, $\Lambda^p F \cong A$ avec action triviale de C_p , si p est impair.

Preuve : Comme F est A -libre de base $1, g, \dots, g^{p-1}$, $\Lambda^k F$ est A -libre de base $g^{i_1} \wedge \dots \wedge g^{i_k}$, $0 \leq i_1 < \dots < i_k \leq p-1$. On met au besoin un signe devant certains éléments en sorte que l'image sous l'action de g d'un vecteur de base soit encore un vecteur de base. Plus précisément, on garde le signe + partout si k est impair et on prend $(-1)^{\sum i_j} g^{i_1} \wedge \dots \wedge g^{i_k}$, $0 \leq i_1 < i_2 < \dots < i_k \leq p-1$, comme base lorsque k est pair. Avec ce choix, C_p agit sur l'ensemble E des éléments de base. Les orbites peuvent avoir 1 ou p éléments. Comme aucun élément de base n'est laissé fixe par g si $0 < k < p$, toutes les orbites ont p éléments. Les éléments d'une orbite engendrent un sous-module libre de rang 1 de $\Lambda^k F$ et il s'ensuit que $\Lambda^k F$ est somme directe de modules libres de rang 1, en nombre $\binom{p}{k}/p$ car $\Lambda^k F$ est A -libre de rang $\binom{p}{k}$. Si maintenant $k = p$, l'unique élément de base $1 \wedge g \wedge \dots \wedge g^{p-1}$ est laissé fixe par g car p est impair et donc $\Lambda^p F \cong A$ avec action triviale de C_p . $\square$

Lemme 5.8 : $\Psi_k[F] = \begin{cases} [F] & \text{si } k \not\equiv 0 \pmod{p} \\ p[A] & \text{si } k \equiv 0 \pmod{p} \end{cases}$

Preuve : Si $p = 2$, soit A_- la représentation signe de C_2 , qui est isomorphe à l'idéal d'augmentation de AC_2 . On a $[F] = [A] + [A_-]$ et donc, comme A et A_- sont de rang 1 et que $[A_-]^2 = [A]$, $\Psi_k[F] = [A]^k + [A_-]^k =$

$$= \begin{cases} [A] + [A] = 2[A] & \text{si } k \text{ est pair} \\ [A] + [A_-] = [F] & \text{si } k \text{ est impair} \end{cases}$$

On suppose maintenant p impair et on raisonne par récurrence sur k .

Pour $k = 1$, on a $\Psi_1 = \text{id}$. Si $1 < k < p$, la définition par récurrence de Ψ_k donne $\Psi_k [F] = [F] \cdot [F] - [F] \cdot \binom{p}{2} / p [F] + \dots + (-1)^k [F] \cdot \binom{p}{k-1} / p [F] + (-1)^{k+1} k \cdot \binom{p}{k} / p [F]$ et comme $[F]^2 = p[F]$, on en tire :

$$\Psi_k [F] = \left(p \binom{p}{2} + \binom{p}{3} - \dots + (-1)^k \binom{p}{k-1} + (-1)^{k+1} k \cdot \binom{p}{k} / p \right) [F].$$

Montrons par récurrence sur k que le coefficient de $[F]$ vaut 1.

Si $k = 2$, $p - 2 \binom{p}{2} / p = p - (p-1) = 1$.

Si $2 < k < p$, l'hypothèse de récurrence appliquée aux $(k-2)$ premiers termes donne :

$$\begin{aligned} & \left[p - \binom{p}{2} + \dots + (-1)^{k-1} \binom{p}{k-2} \right] + (-1)^k \binom{p}{k-1} + (-1)^{k+1} k \cdot \binom{p}{k} / p = \\ & = \left[1 - (-1)^k (k-1) \binom{p}{k-1} / p \right] + (-1)^k \binom{p}{k-1} + (-1)^{k+1} k \binom{p}{k} / p. \end{aligned}$$

Il suffit de montrer que la somme des trois derniers termes est nulle, c'est-à-dire, en multipliant par $(-1)^{k+1} p$, que $(k-1) \binom{p}{k-1} - p \binom{p}{k-1} + k \binom{p}{k} = 0$. Or ceci est clair, car :

$$k \binom{p}{k} = k \binom{p}{k-1} \frac{p-k+1}{k} = (p-(k-1)) \binom{p}{k-1}.$$

Ainsi $\Psi_k [F] = [F]$ si $k < p$.

Si $k = p$, le terme $\Lambda^p F \cong A$ intervient comme dernier terme dans la formule récurrente et on a donc :

$$\Psi_p [F] = \left(p - \binom{p}{2} + \binom{p}{3} - \dots - \binom{p}{p-1} \right) [F] + p \cdot [A]$$

Or $p - \binom{p}{2} + \dots - \binom{p}{p-1} = (-1+1)^p = 0$ car p est impair et donc $\Psi_p [F] = p \cdot [A]$.

Si $k > p$, tous les termes $\Lambda^i F$ sont nuls si $i > p$, et donc

$$\begin{aligned} \Psi_k [F] &= \Psi_{k-1} [F] \cdot \lambda^1 [F] - \Psi_{k-2} [F] \cdot \lambda^2 [F] + \dots - \Psi_{k-p+1} [F] \cdot \lambda^{p-1} [F] + \\ &+ \Psi_{k-p} [F] \cdot \lambda^p [F]. \end{aligned}$$

Or, si $j < k$, $\Psi_j [F] \cdot [F] = p[F]$ indépendamment de la congruence de $j \bmod p$:

Si $j \not\equiv 0 \bmod p$, $\Psi_j [F] \cdot [F] = [F]^2 = p[F]$ et si $j \equiv 0 \bmod p$, $\Psi_j [F] \cdot [F] = p[A] \cdot [F] = p[F]$. Il en résulte que la somme des $(p-1)$ premiers termes ne dépend pas de k et est égale à $\left(p - \binom{p}{2} + \binom{p}{3} - \dots - \binom{p}{p-1} \right) [F] = 0$, comme ci-dessus.

Finalement $\Psi_k [F] = \Psi_{k-p} [F] \cdot \lambda^p [F] = \Psi_{k-p} [F] = \begin{cases} [F] & k \not\equiv 0 \bmod p \\ p[A] & k \equiv 0 \bmod p \end{cases}$. $\square$

Remarque : Cette preuve est valable en fait pour un anneau commutatif A quelconque.

Il nous reste à calculer les $\psi_k[M]$ pour M irréductible de type 1. Or on dispose d'un "splitting principle" particulièrement simple pour ces modules. Soit $\bar{A}$ l'unique p -anneau court non ramifié de longueur r et de corps résiduel la clôture algébrique $\bar{K}$ de K , K étant le corps résiduel de A . L'inclusion $K \subset \bar{K}$ se relève en une injection $h : A \rightarrow \bar{A}$, même unique lorsque K est parfait, en vertu de la proposition 1.18. Par extension des scalaires à $\bar{A}$, tout $\bar{A}C_p$ -module de type 1 se décompose dans $R_{\bar{A}}(C_p)$ en somme d'éléments de rang 1. En effet, un $\bar{A}C_p$ -module irréductible de type 1 est de la forme M_f , où f est un polynôme irréductible sur $\bar{K}$, et comme $\bar{K}$ est algébriquement clos, f est de degré 1 et donc M_f est de rang 1. Pour que ce splitting principle soit opérant, il faut encore que l'extension des scalaires soit injective :

Lemme 5.9 : Si p est impair ou si $r \geq 3$, $h_* : R_A(C_p) \rightarrow R_{\bar{A}}(C_p)$ est injective.

Preuve : Sous les hypothèses faites, $R_{\bar{A}}(C_p)$ est abélien libre sur $[F]$ et sur les classes $[M_f]$ des modules irréductibles de type 1. On a $h_*[F] = [\bar{F}]$ où $\bar{F} = \bar{A}C_p$ et il s'agit essentiellement d'étudier l'extension des scalaires d'un module irréductible M_f de type 1. Par définition de M_f , $p^{r-1}M_f$ est un $K[Y]$ -module simple isomorphe à $K[Y]/(f)$. Par la proposition 4.29, $p^{r-1}(\bar{A} \otimes_A M_f) \cong \bar{K} \otimes_K p^{r-1}M_f$ comme $\bar{K}[Y]$ -modules. Comme les facteurs simples de $\bar{K} \otimes_K K[Y]/(f)$ sont isomorphes à $K[Y]/(g)$ où g est un facteur linéaire de f , les facteurs irréductibles de $\bar{A} \otimes_A M_f$ sont de la forme $\bar{M}_g$, où $\bar{M}_g$ est le $\bar{A}C_p$ -module irréductible de type 1 correspondant au polynôme g . Si donc $f = \prod_j (Y - a_j)^{p^e}$ dans $\bar{K}$, p^e étant le degré d'inséparabilité de f , $h_*[M_f] = \sum_j p^e [M_{Y-a_j}]$.

Soit $x \in R_A(C_p)$ tel que $h_*x = 0$. $x = n[F] + \sum_{i=1}^s n_i[M_{f_i}]$, $n, n_i \in \mathbb{Z}$, et les f_i étant des polynômes irréductibles sur K distincts. Si $f_i = \prod_{j=1}^{k_i} (Y - a_{ij})^{p^{e_i}}$, $h_*x = n[F] + \sum_{i=1}^s \sum_{j=1}^{k_i} n_i p^{e_i} [M_{Y-a_{ij}}]$. Comme $a_{ij} \neq a_{kl}$ si $i \neq k$ vu que leurs polynômes minimaux sur K f_i et f_k sont distincts et que $a_{ij} \neq a_{il}$ si $j \neq l$ vu que ce sont par définition des racines distinctes de f : la relation $h_*x = 0$ implique $n = 0$ et $n_i p^{e_i} = 0$ car $R_{\bar{A}}(C_p)$ est abélien libre. Il en résulte que $n_i = 0$ et donc que $x = 0$. $\square$

Remarque : h_* n'est en général pas injectif dans le cas $p = 2$, $r = 2$. On a vu en effet que $R_A(C_p)$ est toujours abélien libre alors que $R_A(C_2)$ peut avoir de la 2-torsion. L'image par h_* de la 2-torsion ne peut être que nulle.

Théorème 5.10 : On suppose p impair ou $r \geq 3$. Soit $\rho_k : C_p \rightarrow C_p$ l'homomorphisme défini par $\rho_k(g) = g^k$. Soit $\rho_k^* : R_A(C_p) \rightarrow R_A(C_p)$ l'homomorphisme induit.

Alors $\Psi_k = \rho_k^*$. En particulier les Ψ_k sont périodiques en k de période p et

$\Psi_{kp}[M] = [M_0]$ où M_0 est le AC_p -module égal à M comme A -module et muni de l'action triviale de C_p .

Preuve : On vérifie aisément que $\rho_k^*[F] = [F]$ si $k \not\equiv 0 \pmod p$ et que $\rho_k^*[F] = [F_0] = [pA]$ si $k \equiv 0 \pmod p$. Par conséquent $\Psi_k[F] = \rho_k^*[F]$ pour tout k en vertu du lemme 5.8. Pour les modules irréductibles de type 1, on utilise le splitting principe du lemme 5.9 : comme h^* est injective et que Ψ_k aussi bien que ρ_k^* commutent à h_* , il suffit de montrer l'égalité $\Psi_k = \rho_k^*$ dans $R_A(C_p)$. Soit alors $f = Y - a \in \overline{K}[Y]$ et M_f le module irréductible de type 1 correspondant. Comme M_f est de rang 1, $\Psi_k[M_f] = [M_f]^k$ et il reste donc à calculer les puissances tensorielles de M_f . On a $p^{r-1}M_f \cong \overline{K}$ muni de l'endomorphisme de multiplication par a car $p^{r-1}M_f \cong \overline{K}[Y]/(Y-a)$. $p^{r-1}(M_f \otimes_A M_f) \cong p^{r-1}M_f \otimes_{\overline{K}} p^{r-1}M_f$ muni de l'endomorphisme $Y \otimes 1 + 1 \otimes Y$, c'est-à-dire $\overline{K}$ muni de l'endomorphisme de multiplication par $2a$, via l'isomorphisme $\overline{K} \otimes_{\overline{K}} \overline{K} \cong \overline{K}$. On a donc $\overline{K}[Y]/(Y-a) \otimes_{\overline{K}} \overline{K}[Y]/(Y-a) \cong \overline{K}[Y]/(Y-2a)$, ce qui est un cas particulier de la formule générale d'Hannula mentionnée au chapitre 4, §6. Il en résulte que $M_f \otimes_A M_f \cong M_{Y-2a}$, et, par récurrence sur k , que $M_f^{\otimes k} \cong M_{Y-ka}$.

Relevons à $e \in \overline{K}$ un élément de $\overline{A}$ noté encore a . Si C_p est engendré par g , on a, par définition de l'endomorphisme caractéristique de M_f , $(g-1)x = Yp^{r-1}x = p^{r-1}ax$, $x \in M_f$. Donc $M_f \cong \overline{A}$ muni de l'action de g de multiplication par $1 + p^{r-1}a$. De même $M_{Y-ka} \cong \overline{A}$, g agissant par multiplication par $1 + p^{r-1}ka$.

g^k agit sur M_f par multiplication par $(1+p^{r-1}a)^k = 1+p^{r-1}ka$, car $p^r = 0$. Il en résulte que $M_{Y-ka} \cong \rho_k^* M_f$ et donc $M_f^{\otimes k} \cong \rho_k^* M_f$, ce qui montre que $\Psi_k = \rho_k^*$.

Le reste des affirmations s'ensuit de manière immédiate.

ρ_k ne dépend que de la congruence de k mod p et donc les χ_k sont périodiques de période p . $\rho_p(g) = g^p = 1$ et par conséquent g agit par l'identité sur $\rho_p^* M$, c'est-à-dire $\rho_p^* M \cong M_0$. $\square$

Remarque : On a vu que, dans le cas non-modulaire, on a aussi $\chi_k = \rho_k^*$ si le groupe est abélien. Il est fort possible que ce résultat se généralise au cas modulaire. En particulier, il est probable qu'il soit vrai dans le cas $G = C_2$ et $r = 2$ qu'on a laissé de côté dans le théorème.

BIBLIOGRAPHIE

- [Ag] Agou S. : Irréductibilité des polynômes $f(x^p - ax)$ sur un corps fini F_p , J. reine angew. Math. 292(1977), 191-195.
- [Bour] Bourbaki N. : Algèbre commutative, chap. I-IV, Hermann.
- [Bouv] Bouvier A. : Sur les anneaux principaux, Acta Math. Acad. Sci. Hungar. 27 (1976), no 3-4, 231-242.
- [Co] Cohen I. : On the structure and ideal theory of complete local rings, Trans. Amer. Math. Soc. 59 (1946), 54-106.
- [CK] Cohen I, Kaplanski I. : Rings for which every module is a direct sum of cyclic modules, Math. Z. 54 (1951), 97-101.
- [CR] Curtis C, Reiner I. : Representation theory of finite groups and associative algebras, Interscience, 1962.
- [Do] Dornhoff L. : Group representation theory, Dekker, 1972.
- [DL] Drobotenko V.S., Lihtman A.I. : On representations of finite groups over a ring of residue classes mod p^s , Dokl. Soobsč. Užgorodsk. Gos. Univ. Ser. Fiz. Mat. Nauk. no 3, 63 (1960).
- [DDZP] Drobotenko V.S., Drobotenko E.S., Zhilinskaya Z.P., Pogorilyak E.V. : Representations of cyclic groups of prime order over rings of residue classes mod p^s , Amer. Math. Soc. Translations 69, 241-256.
- [Fr] Fröhlich A. : The representation of a finite group as a group of automorphisms on a finite abelian group, Quart. J. Math. Oxford Ser. (2) 1 (1950), 270-283.
- [Gi] Giorgiutti I. : Groupes de Grothendieck, Ann. Fac. Sci. Univ. Toulouse 26 (1962), 151-207.
- [Go] Gorenstein D. : Finite groups, Harper and Row, 1968.
- [GDL] Gudivok P.M., Drobotenko V.S., Lihtman A.I. : On representations of finite groups over the ring of residue classes mod m , Ukrain. Mat. Ž. 16 (1964), 82-89.

- [HR] Heller A., Reiner I. : Representations of cyclic groups in rings of integers, Ann. Math. 76 (1962), 73-92.
- [Ha] Hannula T. : 1. Group representations over integers modulo a prime power, Ph. D. thesis, Univ. of Illinois, 1967.
2. The integral group ring of $(R_K G)$, Trans. Amer. Math. Soc. 133 (1968), 553-559.
- [HS] Hilton P.J., Stammach U. : A course in homological algebra, GTM Springer, 1970
- [Ka] Kervaire M. : Opérations d'Adams en théorie de la représentation des groupes finis, Ens. Math. 22 (1976), 1-28.
- [Kr] Kratzer C. : Opérations d'Adams en K-théorie algébrique, thèse de doctorat, Univ. de Lausanne, à paraître.
- [La] Lazard M. : Détermination des anneaux p-adiques et π -adiques dont les anneaux de restes sont parfaits, séminaire Krasner, 1953-54, exposé 9.
- [Ma] Mac Lane S. : Subfields and automorphism groups of p-adic fields, Ann. Math. 40 (1939), 423-442.
- [Ri] Rim D.S. : Modules over finite groups, Ann. Math. 69 (1959), 700-712.
- [Se] Serre J.P. : 1. Corps locaux, Act. Sci. Ind. 1296 (1962), Hermann.
2. Représentations linéaires de groupes finis, 2ème éd., Hermann, 1971.
- [Sh] Shoda K. : Über die Automorphismen einer endlichen abelschen Gruppe, Math. Ann. 100(1928), 674-686.
- [Sw] Swan R. : A splitting principle in algebraic K-theory, Proc. Symp. in Pure Math. 21 (1971), 155-159.
- [Sz] Szekeres G. : Determination of a certain family of finite metabelian groups, Trans. Amer. Math. Soc. 66 (1949), 1-43.
- [Wa] Warfield R.A. : Rings whose modules have nice decompositions, Math. Z. 125 (1972), 187-192.
- [ZS] Zariski O., Samuel P. : Commutative algebra, van Nostrand, 1958.

